

werts nach § 35 Abs. 1a Nr. 3 GWB in der Fusionskontrolle erscheint es hingegen zumindest zweckmäßig, eine vorherige positive Evaluation abzuwarten.

#### V. Zusammenfassung

- 44 1. Mit den §§ 18 Abs. 2a und Abs. 3a, 35 Abs. 1a GWB durchbricht der deutsche Gesetzgeber die bisherige, im deutschen Kartellrecht bestehende, insbesondere auf den *more economic approach* zurückzuführende Fixierung auf Preise und Entgeltlichkeit. Mit der Einführung dieser Regelungen zeigt der deutsche Gesetzgeber, dass er bereit ist, auf neue wirtschaftliche Entwicklungen, wie sie insbesondere durch die Internetökonomie eingetreten sind, zu reagieren.
- 45 2. § 18 Abs. 2a und Abs. 3a GWB gelten trotz ihrer systematischen Stellung bei der Definition der Marktbeherrschung für das gesamte GWB. Auch wenn diese beiden neuen Absätze keine grundlegenden Neuerungen mit sich bringen, so haben diese Regelungen doch jedenfalls Signalwirkung dahin, dass sich auch der Rechtsanwender neueren ökonomischen Entwicklungen und Erkenntnissen nicht verschließen darf.
3. Mit der Einführung des Wertes der Gegenleistung als Aufgreifkriterium für die Fusionskontrolle in § 35 Abs. 1a Nr. 3 GWB betritt der deutsche Gesetzgeber fragwürdiges und schwieriges Neuland in Europa.
- 47 4. In den europäischen Wettbewerbsregeln ist eine Modernisierung wie im GWB durch Regelungen wie §§ 18 Abs. 2a und Abs. 3a, 35 Abs. 1a GWB bisher nicht zu finden. Es liegen bis auf eine sehr vage Mitteilung der Kommission zu digitalen Plattformen noch nicht einmal Regelungsvorschläge vor.
- 48 5. Die europäischen Wettbewerbsregeln täten gut daran, einen *more new economic approach* zu verfolgen, um auf dem europäischen Binnenmarkt auch unter den geänderten wirtschaftlichen, insbesondere digitalen Rahmenbedingungen, im Interesse eines funktionierenden Binnenmarktes wirksamen Wettbewerb zu gewährleisten. Die hierzu ins GWB neu eingeführten Regelungen des § 18 Abs. 2a und Abs. 3a GWB können hierfür Vorbild sein. Im Hinblick auf das neue Aufgreifkriterium des Transaktionswerts nach § 35 Abs. 1a Nr. 3 GWB in der Fusionskontrolle erscheint es hingegen zweckmäßig, zumindest eine vorherige positive Evaluation abzuwarten.

Prof. Dr. Thomas Hoeren, Münster und Dr. Reiner Münker, Bad Homburg\*

## Die EU-Richtlinie für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung – unter besonderer Berücksichtigung der Produzentenhaftung

### INHALT

- I. Einführung
- II. Regulierungsziele
- III. Der Begriff des Geschäftsgeheimnisses
- IV. Das Zentralverbot
- V. Die erweiterte Haftung des Herstellers
- VI. Ausnahmen und Beschränkungen
  1. Schranken und tatbestandsausschließende Merkmale (Art. 3)
  2. Ausnahmen und Rechtfertigungsgründe (Art. 5)
- VII. Sanktionen
- VIII. Fazit

- 1 Im Juni 2018 endet die Umsetzungsfrist für ein Gesetz zur Neuregelung der Geschäftsgeheimnisse. Die Autoren beschreiben die zugrunde liegende EU-Richtlinie (RL (EU) 2016/943, nachfolgend „Richtlinie“) für den Schutz von Geschäftsgeheimnissen und skizzieren deren Umsetzungsmöglichkeiten. Besonderes Augenmerk gilt dabei der Produzentenhaftung nach Art. 4 Abs. 5 der Richtlinie.

#### I. Einführung

- 2 Es gibt viele Wege, wie wertvolles Wissen aus dem Unternehmen entweichen kann. Mitarbeiter mit Spezialwissen verlassen das Unternehmen, Cyberattacken können ebenfalls der Fall sein sowie Abfotografieren, Abspeichern oder andere Formen der Preis-

gabe durch Mitarbeiter. Auch E-Mails können abgefangen und mitgelesen werden. Der geschätzte Schaden durch Wirtschaftsspionage beträgt in Deutschland jährlich rund 50 Milliarden Euro. International haben die Industriestaaten durch Art. 39 Abs. 2 des TRIPS-Abkommens Vorsorge getroffen. Als Mindeststandard haben sich die Mitgliedstaaten von TRIPS verpflichtet, Informationen gegen den unberechtigten Abgang zu schützen, solange diese Informationen geheim sind, d. h.

- in der Zusammenstellung in üblichen Geschäftskreisen nicht allgemein bekannt oder zugänglich sind,
- einen wirtschaftlichen Wert haben, weil sie geheim sind, und
- Gegenstand von angemessenen Geheimhaltungsmaßnahmen darstellen.

In Deutschland besteht ein besonderer Schutz für Geschäftsgeheimnisse durch die traditionell strafrechtlichen Vorschriften in §§ 17 bis 19 UWG. Die Straftatbestände werden über Transfernormen auch zivilrechtlich sanktioniert (§ 3 UWG, § 823 Abs. 2 BGB). Diese UWG-Normen existierten schon, als es das TRIPS-Abkommen noch nicht gab. Dementsprechend sind die Regulierungsziele von TRIPS und §§ 17 bis 19 UWG nicht identisch. Neu sind vor allem besondere Nachweisproblematiken für den Geheimnischarakter der Information und die Nachweispflichten für angemessene Geheimhaltungsvereinbarungen. In der europäischen Übersicht liegt Deutschland im Mittelfeld des Schutzniveaus von Geheimnissen. Während Großbritannien über ein wohlgedachtes System von Geheimhaltungspflichten verfügt, sind in Staaten wie Frankreich oder Malta Geheimhaltungsvereinbarungen nahezu unbekannt. Dies hat die Kommission schon im November 2011 und April 2013 bewogen, zwei Studien

\* Mehr über die Autoren erfahren Sie auf S. 259.

## Hoeren/Münker, Die EU-RL für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung

zum Schutz von Geschäftsgeheimnissen im europäischen Vergleich in Auftrag zu geben. Die Studien kamen naturgemäß zu der Feststellung, dass der Geheimnisschutz in Europa einem Flickenteppich ähnelt.<sup>1)</sup> Die Kommission hat daraufhin im November 2013 einen ersten Entwurf für eine Harmonisierungsrichtlinie verabschiedet.<sup>2)</sup> Im Mai 2014 folgte der gemeinsame Text, verabschiedet vom Ministerrat.<sup>3)</sup> Ein Jahr später – im Juni 2015 – legte das Parlament seinen Bericht zum Richtlinienentwurf vor,<sup>4)</sup> auf dessen Grundlage die Europäische Kommission, der Rat und das Parlament im Rahmen (inoffizieller) Trilog-Verhandlungen einen Kompromissvorschlag erarbeiteten, der im Dezember 2015 veröffentlicht wurde.<sup>5)</sup> Im Juni 2016 konnte schließlich die Richtlinie verabschiedet werden,<sup>6)</sup> die nunmehr bis Juni 2018 in das nationale Recht umzusetzen ist.<sup>7)</sup> Jetzt wird auf nationaler Ebene darüber gestritten, ob der Schutz von Geschäftsgeheimnissen in ein umfassendes eigenes Regelwerk für Immaterialgüterrechte aufzunehmen ist<sup>8)</sup> oder zumindest ein Spezialgesetz die Thematik regeln sollte.<sup>9)</sup> In Deutschland hat die Unterbrechung durch die Bundestagswahl zur Diskontinuität eventueller Vorentwürfe der alten Koalition geführt: Jedenfalls muss das Bundesjustizministerium (BMJV) von Neuem einen Entwurf in die parlamentarische Diskussion einbringen. Sicher ist schon jetzt, dass die Umsetzungsfrist bis Juni 2018 nicht eingehalten werden kann. Wie man hört, plant das Ministerium die Umsetzung in ein eigenes Spezialgesetz, allerdings ohne § 17 UWG anzutasten.<sup>10)</sup> Ein interner Entwurf, an dem neben dem BMJV auch das Arbeits- und Wirtschaftsministerium mitgewirkt haben, liegt bereits seit einem Jahr vor. Er sieht eine direkte Umsetzung der Richtlinie in nationales Recht vor; kann allerdings bei Bedarf um weitere Elemente ergänzt werden.

## II. Regulierungsziele

- 4 Die Richtlinie beabsichtigt, die existierenden verschiedenen nationalen Regelungen zu harmonisieren.<sup>11)</sup> Angedacht ist die Einordnung als ergänzende oder alternative Maßnahme zu Immaterialgüterrechten (Erwägungsgrund 2). Das Verhältnis zum UWG

wird generell offengelassen und einer späteren Prüfung durch die Kommission anheimgegeben (Erwägungsgrund 10). Im Übrigen soll die Richtlinie jetzt<sup>12)</sup> nur eine Mindestharmonisierung beinhalten (Art. 1 Abs. 1). Auch zu berücksichtigen ist, dass die EU keine Zuständigkeit für das Strafrecht hat und außerdem nicht in Anspruch nimmt, eine Regelung zum Betriebsverfassungsrecht oder Presserecht vorzunehmen (Art. 1 Abs. 2). Verblüffend ist, dass die Richtlinie keine Regelung zum Internationalen Privatrecht (IPR) enthält. Angeknüpft werden könnte an das Strafrecht, das Immaterialgüterrecht oder das UWG. Letztendlich rächt sich hier, dass die Rechtsnatur des neu geschaffenen Systems unklar ist. Ordnet man das System immaterialgüterrechtlich ein, greift die Richtlinie schon bei jeder Benutzungshandlung mit Bezug zur EU. Nach dem UWG wäre stattdessen nach dem finalen Markteingriff oder der bestimmungsgemäßen Benutzung zu fragen.

## III. Der Begriff des Geschäftsgeheimnisses

Dreh- und Angelpunkt der Richtlinie ist der Begriff des Geschäftsgeheimnisses.<sup>13)</sup> Er ist weit gefasst, weiter als nach § 17 UWG.<sup>14)</sup> Ein Geheimnis soll schon vorliegen, wenn die Information generell unbekannt oder in den angesprochenen Verkehrskreisen nicht bekannt ist.<sup>15)</sup> Unklar ist, welche Kreise als angesprochene Verkehrskreise betrachtet werden. Auch die Existenz eines Außenseiters oder eines Hackers macht rein faktisch die Information zugänglich. Das Problem ist allerdings nicht neu, sondern war schon bei § 17 UWG bekannt. Die Rechtsprechung hat darauf abgestellt, dass die Erschließung einer Information einen großen Zeit- und Kostenaufwand erfordert und hat hierfür ebenfalls auf die Sicht der Fachkreise abgestellt.<sup>16)</sup> Zudem muss das Geschäftsgeheimnis einen kommerziellen Wert verkörpern, weil es geheim ist (Art. 2 Ziff. 1 lit. b). Der Wert des Geschäftsgeheimnisses muss also gerade im Geheimnis liegen.<sup>17)</sup> Dies ist für deutsche Leser gänzlich unbekannt, da nach § 17 UWG weder nach dem Wert der Information noch nach dem Vorliegen eines Geheimnisses gefragt wird. Das deutsche Recht hat stattdessen stets auf das Erfordernis eines objektiv bestehenden, wirtschaftlichen Geheimhaltungsinteresses abgestellt und insofern auch Geheimnisse ohne Wert geschützt, deren Bekanntwerden Schaden verursachen könnte.<sup>18)</sup> Die Definition stammt aus Art. 39 TRIPS. Nunmehr wird es also erforderlich sein, die Werthaltigkeit einer Information gerichtsfest dokumentieren zu können.<sup>19)</sup>

Das setzt zum einen eine Bilanzierung von Geschäftsgeheimnissen voraus. Zum anderen ist der Nachweis der Geheimhaltung als Status quo zu erbringen. Schon bei diesem Element wird man also ein umfassendes Geheimnismanagement nachweisen müssen, das bis zur Verschlüsselung von E-Mails und IT-Sicherheit geht.<sup>20)</sup>

1) Study on Trade Secrets and Confidential Business Information in the Internal Market, MARKT/2011/128/D (April 2013), 12 f., 23, abrufbar unter: [http://ec.europa.eu/internal\\_market/iprenforcement/docs/trade-secrets/130711\\_final-study\\_en.pdf](http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf).  
 2) Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, COM/2013/0813 final – 2013/0402 (COD), abrufbar unter: <http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A52013PC0813>.  
 3) Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure – General Approach, abrufbar unter: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209870%202014%20INIT>.  
 4) Bericht über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, abrufbar unter: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2015-0199+0+DOC+XML+V0//DE>.  
 5) Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure – Analysis of the final compromise text with a view to agreement, abrufbar unter: <http://data.consilium.europa.eu/doc/document/ST-15382-2015-REV-1/en/pdf>.  
 6) RL 2016/943/EU v. 08.06.2016, ABl. L 157/1 v. 15.06.2016, abrufbar unter: <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L0943>.  
 7) *Kalbfus*, GRUR 2016, 1009; *Ann*, GRUR-Prax 2016, 465.  
 8) *So McGuire*, GRUR 2016, 1000, 1007 f. mit Verweis auf Italien und Portugal.  
 9) *So etwa in Schweden: Act on the Protection of Trade Secrets (1990)*, abrufbar unter: [http://www.wipo.int/wipolex/en/text.jsp?file\\_id=241716](http://www.wipo.int/wipolex/en/text.jsp?file_id=241716); vgl. auch AIPPI Report Q 215 (2010); *Tonell*, in: Källezi/Kilpatrick/Kobel, Abuse of Dominant Position and Globalization & Protection and Disclosure of Trade Secrets and Know-How 2017, S. 541 ff.  
 10) Anders allerdings *McGuire*, GRUR 2016, 1000, 1008, die selbstverständlich davon ausgeht, dass § 17 UWG aufgehoben oder geändert werden muss. *Kalbfus*, GRUR 2016, 1009, 1016 plädiert dafür, ein Stammgesetz mit den zivilrechtlichen Regelungen vorzubehalten und das Strafrecht für besonders eklatante, insbesondere vorsätzliche Verletzungsformen in dieses Stammgesetz zu integrieren.  
 11) *Ann*, GRUR-Prax 2016, 465; *Koós*, MMR 2016, 224.

12) Anders noch der Kommissionsentwurf, COM/2013/0813 final – 2013/0402 (COD) (Fn. 2), vgl. dazu *Kalbfus/Harte-Bavendamm*, GRUR 2014, 453.  
 13) *Klein/Wegener*, GRUR-Prax 2017, 394.  
 14) *Kalbfus*, GRUR 2016, 1009, 1011 f. vertritt eine etwas andere These, wonach die deutsche Rechtsprechung zu § 17 UWG im Kern den Vorgaben der Richtlinie entspricht. Trotzdem hält er eine Umsetzung der Richtlinie in ein spezielleres deutsches Gesetz für geboten.  
 15) *McGuire*, GRUR 2016, 1000 mit dem Kernvorschlag, den Geheimnisschutz in das System des geistigen Eigentums einzubetten.  
 16) BGH, 12.02.1980 – KZR 7/79, WRP 1980, 403, 404 – Pankreaplex II; BGH, 23.02.2012 – I ZR 136/10, WRP 2012, 1230, 1232, Rn. 21 – MOVICOL-Zulassungsantrag.  
 17) *Sousa e Silva*, Journal of Intellectual Property Law & Practice 2014, 923.  
 18) *Kalbfus*, GRUR 2016, 1009, 1011.  
 19) *So auch Herrmann*, CB 2016, 368, 369.  
 20) *Pacini/Placida/Wright-Isak*, Int. Journal of Law and Management 2008, 121, mit Präsentation eines „trade secret compliance plans“ inklusive unterschiedlicher Maßnahmen, die ergriffen werden können sowie unterschiedlicher Variablen auf die je nach Unternehmen geachtet werden muss.

## Hoeren/Münker, Die EU-RL für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung

7 Damit nicht genug: Es muss auch der Nachweis erbracht werden, dass das Geheimnis Gegenstand von angemessenen Schritten zur Geheimhaltung ist (Art. 2 Ziff. 1 lit. c). Es bedarf also auch proaktiver kontinuierlicher Geheimhaltungsmaßnahmen, um den Geheimnischarakter einer Information bewahren zu können. Dies setzt umfangreiche und vor allem langfristige Maßnahmen voraus, die dem neuesten Stand der Technik entsprechen.<sup>21)</sup> Für deutsche Betroffene ist es neu, dass angemessene Geheimhaltungsmaßnahmen Schutzvoraussetzung sind. Sie spielten bisher allenfalls im Beweisrecht eine Rolle. Der BGH hatte es bislang ausreichen lassen, dass sich ein Geheimhaltungswille aus der Natur der Sache ergibt, und hat selbst das Fehlen ausdrücklicher Geheimhaltungsvereinbarungen als unproblematisch angesehen.<sup>22)</sup> Daher aber machen sich viele Gedanken darüber, was unter der Angemessenheit von Geheimhaltungsmaßnahmen zu verstehen ist.<sup>23)</sup> In der Richtlinie wird der Begriff nicht näher erläutert. Vorausgesetzt werden nicht bestmögliche oder maximal effektive Schutzvorkehrungen, sondern nur ein angemessener Schutzstandard.<sup>24)</sup> Für die unternehmensinterne Umsetzung sind daher konkrete Schritte zu bestimmen. Zunächst gilt es, klare Zuständigkeiten für den Schutz von Geschäftsgeheimnissen im Unternehmen zu definieren. Anschließend muss das potentiell relevante Know-how identifiziert und nach Unternehmensgröße und Branche bewertet und kategorisiert werden. Schließlich müssen konkrete Schutzmaßnahmen festgelegt werden, einschließlich besonderer Vertragsvereinbarungen, Maßnahmen der IT-Sicherheit und der Organisation von Arbeitsabläufen.<sup>25)</sup> In der Automobilindustrie wird zum Beispiel darauf geachtet, dass gebäudetechnische, informationssicherheitstechnische und organisatorische Maßnahmen durchgeführt und über Audits geprüft werden. Die Zertifizierung erfolgt für den Bereich IT-Sicherheit nach IS. 27001.<sup>26)</sup>

8 Offen bleibt auch die dogmatische Frage, ob das Geschäftsgeheimnis nun als subjektives Recht ähnlich den klassischen Immaterialgüterrechten anerkannt ist. Im deutschen Recht ist die Rechtsnatur von Unternehmensgeheimnissen hoch streitig.<sup>27)</sup> Abgestellt wird auf den Zuweisungsgehalt und die Ausschlusswirkung. Diese wird von der herrschenden Meinung für Geheimnisse abgelehnt, da der Geheimnischarakter schnell verloren geht.<sup>28)</sup> Geheimnisschutz soll kein Verwertungsrecht für die Information als solche, sondern nur einen Schutz gegen einen unlauteren Zugang gewähren. So spricht auch Erwägungsgrund 16 der Richtlinie davon, dass die neuen Vorschriften zum Schutz der Innovation und des Wettbewerbs kein exklusives Recht an Know-how oder Informationen, die als Geschäftsgeheimnisse geschützt sind, schaffen. Allerdings spricht auch einiges für einen Charakter der Geschäftsgeheimnisse als kleines Immaterialgüterrecht. Die Präambel charakterisiert in Erwägungsgrund 2 offen den Geheimnisschutz als eine Ergänzung oder eine Alternative zum klassischen gewerblichen Rechtsschutz. Gleichzeitig erklärt Erwägungsgrund 3, dass Geschäftsgeheimnisse eine der häufigsten Formen des Schutzes von geistigen Schöpfungen und

innovativen Know-hows seien. Auch der Umfang der Sanktionsmöglichkeiten spricht für ein kleines Immaterialgüterrecht, das in Anlehnung an die großen Schutzrechte etwa durch dreifache Schadensberechnung geschützt ist. Damit ist das Geschäftsgeheimnis wie ein großes Schutzrecht gesichert.

Nach Art. 2 Ziff. 2 ist Inhaber des Geschäftsgeheimnisses diejenige natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis ausübt. Entscheidend ist also nicht der Schöpfer, sondern derjenige, der die rechtmäßige Kontrolle ausübt. Unklar ist, was unter Kontrolle zu verstehen ist. Stellt man hier auf die tatsächliche Zugriffsmöglichkeit ab, wäre der Arbeitnehmer originärer Inhaber, solange der Arbeitgeber die Informationen nicht bekommen hat. In der Richtlinie steht der Schutz der Unternehmen aber im Zentrum; deshalb finden sich dort auch keine Regeln für den derivativen Erwerb. Durch das Merkmal der angemessenen Schutzmaßnahmen wird ein originärer Erwerb durch den Unternehmer begründet. Damit ergibt sich für die Unternehmen die Pflicht, durch arbeitsvertragliche und betriebliche Anweisungen, Geheimhaltungsstrukturen zu schaffen und damit originäre Erwerbstatbestände zu begründen.<sup>29)</sup>

## IV. Das Zentralverbot

Das Zentralverbot findet sich in Art. 4 Abs. 1 der Richtlinie. Zu beachten ist, dass davor Art. 3 den Grundsatz der Zugangsfreiheit betont. Dementsprechend werden in der Richtlinie zunächst Tatbestände für lautere Geschäftspraktiken aufgezählt. Art. 4 enthält jedenfalls nur Ausnahmen, in denen der Grundsatz der Zugangsfreiheit in bestimmten Konstellationen nicht gilt. Hier nach müssen die Mitgliedstaaten gewährleisten, dass der Geheimnisschutzinhaber alle Maßnahmen und Sanktionsmöglichkeiten zur Verfügung hat, um seine Geheimnisse effektiv vor einem illegalen Erwerb, einer illegalen Nutzung und Offenbarung zu schützen. Diese Maßnahmen werden dann in Art. 4 Abs. 2 und 3 spezifiziert.

Zunächst steht die Aneignung von Geheimnissen im Vordergrund (Art. 4 Abs. 2 lit. a). Der englische Richtlinientext spricht dabei von *acquisition*, was übersetzt wird mit Erwerb. Hier stimmt die offizielle Übersetzung der Richtlinie nicht ganz. Es geht nicht um den (entgeltlichen) Erwerb, sondern um die faktische Aneignung. Die Aneignung ist ohne Zustimmung des Rechteinhabers illegal, wenn weitere Tatbestände vorliegen. Dazu zählt der unautorisierte Zugang oder das Kopieren von Dokumenten, Materialien oder elektronischen Dateien, die das Geheimnis enthalten oder von denen das Geheimnis abgeleitet werden kann.

Diese restriktiven Aneignungsverbote werden dann in Art. 4 Abs. 2 lit. b noch ausgeweitet, in dem jeder andere Tatbestand sanktioniert wird, der ehrlichen geschäftlichen Praktiken entgegensteht. Dieser Tatbestand ist sehr ungenau und kaum zu umgrenzen. Vorgeschlagen wird, ihn über Art. 39 Abs. 2 TRIPS zu konturieren.<sup>30)</sup>

Nicht geregelt ist in der Verbotsliste der Transfer von einzelnen Informationen aus dem Gehirn eines Arbeitnehmers. Wenn ein Arbeitnehmer als Programmierer des Unternehmens Programme im Firmeneigentum liest und den Quellcode speichert, erfüllt dies keinen Verbotstatbestand. Man kann also auch weiterhin<sup>31)</sup> davon ausgehen, dass die Verwendung von Informationen aus

21) *Kalbfus*, GRUR-Prax 2017, 391; *Bürger/Rein*, CB 2017, 118; zur Besonderheit im Automobilbereich *Steinmann/Schubmehl*, CCZ 2017, 194.

22) BGH, 27.04.2006 - I ZR 126/03, WRP 2006, 1511, 1513 - Kundendaten Programm.

23) Siehe etwa *Kalbfus*, Know-how-Schutz in Deutschland zwischen Zivilrecht und Strafrecht - welcher Reformbedarf besteht? 2011, 65 ff.; *Kalbfus*, GRUR-Prax 2017, 391.

24) *Kalbfus*, GRUR-Prax 2017, 391, 392; unzutreffend *Steinmann/Schubmehl*, CCZ 2017, 194, 198, die auf einen rein faktischen Geheimnisschutz abstellen und verkennen, dass die Richtlinie durchaus normative Vorstellungen vom Geheimnisschutz hat.

25) *Kalbfus*, GRUR-Prax 2017, 391, 391 ff.

26) *Steinmann/Schubmehl*, CCZ 2017, 194, 197.

27) Für die Einordnung des Geschäftsgeheimnisses als absolutes Recht s. *Köhler*, in: *Köhler/Bornkamm*, UWG, 35. Aufl. 2017, § 17 Rn. 53; *Nastelski*, GRUR 1957, 1, 6; anderer Ansicht *Ann*, GRUR-Prax 2016, 465; *McGuire*, GRUR 2015, 424, 426; *Hauck*, NJW 2016, 2218, 2221.

28) *Ann*, GRUR-Prax 2016, 465; *McGuire*, GRUR 2015, 424, 426; *Hauck*, NJW 2016, 2218, 2221.

29) *Klein/Wegener*, GRUR-Prax 2017, 394, 396.

30) Siehe *Koós*, MMR 2016, 224, 226.

31) BGH, 03.05.2001 - I ZR 153/99, WRP 2001, 1174, 1176 - Spritzgießwerkzeuge; BGH, 15.03.1955 - I ZR 111/53, GRUR 1955, 424, 425; BAG, 15.06.1993 - 9 AZR 558/91, NZA 1994, 502, 505; BAG, 15.12.1987 - 3 AZR 474/86, NZA 1988, 502, 504.

## Hoeren/Münker, Die EU-RL für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung

dem Gehirn eines Mitarbeiters frei ist. Eventuell kann man aber hier bei bestimmten Missbrauchsfällen Art. 4 Abs. 2 lit. b heranziehen. Allerdings bestimmt Art. 1 Abs. 3 der Richtlinie, dass keine Vorschrift dieser Richtlinie so ausgelegt werden darf, dass sie eine Grundlage dafür bietet, die Mobilität der Arbeitnehmer zu beschränken. Insbesondere bildet die Richtlinie keine Grundlage für Beschränkungen der Nutzung von Erfahrungen und Fähigkeiten, die Arbeitnehmer im normalen Verlauf ihrer Tätigkeit ehrlich erworben haben. Sie stellt auch keine Grundlage für die Auferlegung zusätzlicher vertraglicher Beschränkungen dar.

14 Die Nutzung und Offenbarung von Geheimnissen wird in Art. 4 Abs. 3 der Richtlinie geregelt. Verboten ist die Verwendung von Geschäftsgeheimnissen ohne Zustimmung des Rechteinhabers durch Personen, die sich das Geschäftsgeheimnis illegal angeeignet oder gegen eine Vertraulichkeitsvereinbarung oder sonstige Vertraulichkeitspflicht verstoßen haben. Warum die Richtlinie zwei verschiedene Vertragsverletzungen ins Visier nimmt, ist unklar. Der Tatbestand läuft auf eine Durchsetzung vertraglicher Pflichten mit Mitteln des UWG hinaus. Auf eine Rechtswirksamkeit der Vereinbarung kommt es nicht an. Das Wort *rechts-wirksam*, das ursprünglich in Frühentwürfen der Richtlinie enthalten war, wurde ersatzlos gestrichen.<sup>32)</sup>

15 Neu ist auch, dass schon der objektiv rechtswidrige Eingriff in Art. 4 der Richtlinie für Sanktionen ausreicht. Die ursprünglich im Entwurf vorgesehene Begrenzung von Vorsatz und grober Fahrlässigkeit ist im Endtext nicht mehr enthalten.<sup>33)</sup> Verschulden spielt demnach nur für den Schadensersatz nach Art. 14 der Richtlinie eine Rolle. Auch dies spielt mit dem geltenden deutschen Recht nicht zusammen, das stets ein Verschulden des Anspruchsgegners voraussetzt. Nach der Richtlinie kann der Geheimnisträger jetzt schon bei bloßem Geheimnisbruch Ansprüche auf Unterlassung und Beseitigung geltend machen. Dies entspricht der gegenwärtigen Rechtslage bei einer Verletzung von Immaterialgüterrechten (vgl. § 14 Abs. 5 MarkenG, § 139 Abs. 1 PatG). Folglich erweitert die Richtlinie den Schutz von Geschäftsgeheimnissen und gleicht sie den Immaterialgüterrechten an.

## V. Die erweiterte Haftung des Herstellers

16 Eine weitere Neuregelung enthalten Art. 4 Abs. 4 und Abs. 5 der Richtlinie. Die dort geregelten erweiterten Haftungstatbestände sind dem deutschen Recht im Grundsatz fremd und gerade deshalb gefährlich.

17 Verboten ist hiernach der Erwerb geheimer Informationen durch Dritte, die zum Zeitpunkt des Erwerbs wussten oder fahrlässig nicht wussten, dass unseriöse Geschäftspraktiken an dem Erwerb beteiligt waren (Art. 4 Abs. 4 der Richtlinie). Erstaunlich ist der Hinweis, dass schon die mittelbare Nutzung des fremden Geschäftsgeheimnisses ausreicht. Damit unterscheidet sich das neue System von dem alten des UWG. Aufgrund eines vertraglichen Schutzes können Dritte nach geltendem Recht nur nach Maßgabe von § 17 Abs. 1 oder Abs. 2 Nr. 1 UWG herangezogen werden. Jetzt richtet sich die neue Regelung gegen jeden rechtswidrigen Vorerwerb Dritter. § 17 UWG stellt auch auf schärfere subjektive Elemente (Vorsatz, Absicht) ab als die Richtlinie (Vorsatz oder Fahrlässigkeit).<sup>34)</sup>

18 Nach Art. 4 Abs. 5 ist auch das Herstellen, Anbieten oder Vermarkten rechtsverletzender Produkte oder die Einfuhr, Ausfuhr

oder Lagerung von rechtsverletzenden Produkte für diese Zwecke eine rechtswidrige Nutzung eines Geschäftsgeheimnisses. Dies gilt jedoch nur, wenn die Person, die diese Tätigkeiten durchgeführt hat, Kenntnis von der Tatsache hatte oder den Umständen entsprechend Kenntnis davon hätte haben müssen, dass ein Geschäftsgeheimnis rechtswidrig genutzt wurde. Teilweise sind solche Geheimnisverletzungen durch § 17 Abs. 2 Nr. 2 UWG verboten, da die Herstellung eines Produktes als Verwertung im Sinne der Vorschrift gilt.<sup>35)</sup> Nach der Richtlinie steht auch die Verwendung von Lieferantendaten, von denen der Dritte rechtswidrig Kenntnis erlangt hat, im Zusammenhang mit der Herstellung. Rechtsschutz besteht dann gegen jede Person, die Teil der nachgelagerten Vertriebskette ist, selbst bei Unkenntnis von dem Geheimnis und keiner Verkörperung desselben in dem Produkt.<sup>36)</sup>

## VI. Ausnahmen und Beschränkungen

Soweit die Neuerungen, die schon deutlich über den Tatbestand von § 17 UWG hinausgehen. Kompensatorisch ist der Tatbestand von Schranken und Ausnahmen der Richtlinie im Zuge der Verhandlung exorbitant gewachsen. Solche Beschränkungen finden sich in Art. 3 und Art. 5 der Richtlinie. Ungewohnt ist die Einordnung des Zentralverbots in Art. 4 umgeben von Art. 3 und Art. 5. Unklar ist auch die Abgrenzung der einzelnen Tatbestände. Art. 5 spricht von „Ausnahmen“, während Art. 3 von „rechtmäßigem Erwerb, rechtmäßiger Nutzung und rechtmäßiger Offenlegung“ spricht. Fraglich ist, wie man diese sprachlichen Nuancen bei der Umsetzung wiedergibt. Bei Art. 3 der Richtlinie könnte es sich zum Beispiel um tatbestandsausschließende Merkmale handeln, während die Tatbestände des Art. 5 als Rechtfertigungsgründe in Betracht kommen. Art. 3 wäre als Schranke und Art. 5 als Ausnahme zu verstehen.

### 1. Schranken und tatbestandsausschließende Merkmale (Art. 3)

Art. 3 Abs. 1 lit. a bezeichnet die unabhängige Entdeckung oder Schöpfung als legitim. Der Begriff der Entdeckung verweist auf das Patentrecht, während die Schöpfung eine typische Begrifflichkeit des Urheberrechts ist. Tatsächlich regelt das Patentrecht, für den Fall, dass eine identische Erfindung unabhängig voneinander von mehreren Personen gemacht worden ist, dass das Recht demjenigen zusteht, der die Erfindung zuerst beim Patentamt angemeldet hat (§ 6 S. 3 PatG, Art. 60 Abs. 2 EPÜ). Der Schutz des späteren Anmelders erfolgt dann gegebenenfalls über ein Vorbenutzungsrecht (§ 12 Abs. 1 S. 1 PatG). Im Urheberrecht ist das Phänomen der Doppelschöpfungen ebenfalls bekannt. Es handelt sich nicht um eine Rechtsverletzung, sondern um einen schwarzen Fleck auf der urheberrechtlichen Landkarte und eine bizarre Ausnahmekonstellation, in der beide Urheber ihre Rechte geltend machen können.

Art. 3 Abs. 1 lit. b regelt die allgemeine Testfreiheit. Die Regelung erlaubt die Analyse und das Austesten eines Produkts, das der Öffentlichkeit bekannt gemacht worden ist oder rechtmäßig im Besitz des Erwerbers der Information ist. Hiermit betritt die Richtlinie Neuland. Es geht um eine europäische Regelung zum Reverse Engineering aus dem US-Recht. In Deutschland gilt traditionell das Reverse Engineering als verboten.<sup>37)</sup> Spuren des Reverse Engineering finden sich im Urheberrecht (§§ 69d Abs. 3,

32) *Kalbfus*, GRUR 2016, 1009, 1014 sieht § 18 UWG als Pendant zur Neuregelung und fordert insofern dessen Abschaffung zugunsten einer allgemeinen Regelung für Geschäftsgeheimnisse.

33) Diese Änderung wurde u. a. vom Max Planck Institut gefordert: *Knaak/Kur/Hilty*, International Review of Intellectual Property and Competition Law 2014, 953.

34) Dazu auch *Wiese*, die EU-Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen. Inhalt und Auswirkung auf den gesetzlichen Schutz des Unternehmensgeheimnisses, Dissertation Münster 2017, 141 ff.

35) *Kalbfus*, GRUR 2016, 1009, 1014.

36) *Kalbfus*, GRUR 2016, 1009, 1014.

37) RG, 22.11.1935 – II 128/35, RGZ 149, 329, 331 – Stiefeleisenpresse; vgl. auch OLG Hamburg, 19.10.2000 – 3 U 191/98, GRUR-RR 2001, 137; dazu auch *Beater*, Nachrichten im Wettbewerb – Eine rechtsvergleichende Untersuchung zu Paragraph 1 UWG, 1995, S. 136; *Kochmann*, Schutz des „Know-how“ gegen ausspähende Produktanalysen („Reverse Engineering“), 2009, S. 140.

## Hoeren/Münker, Die EU-RL für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung

69e UrhG) und im Patentrecht (§ 11 Nr. 1 und 2 PatG) ausführlich geregelt. Das Halbleiterschutzgesetz enthält eine ausführliche Erlaubnis für Reverse Engineering (§ 6 Abs. 2 Nr. 2 und 3 HalblSchG). Dort geregelt sind die Nachbildung von Topographien zum Zwecke der Analyse, Bewertung oder Ausbildung sowie die geschäftliche Verwertung einer Topographie, die das Ergebnis einer Analyse oder Bewertung ist. Die Testfreiheit bezieht sich auf ein Produkt, das der Öffentlichkeit zugänglich gemacht worden ist oder sich rechtmäßig im Besitz des Erwerbers der Information befindet. Der Grundsatz geht weit über den Erschöpfungsgrundsatz im Urheberrecht und im Patentrecht hinaus und bezieht sich auch auf vermietete Produkte. Erstaunlich ist ein kleiner Zusatz, wonach der Erwerber der Information frei von rechtlichen Pflichten sein muss, um das Geheimnis zu nutzen. Es ist also vertraglich zulässig, die Testfreiheit zu beschränken. In Lieferverträgen sowie Kooperationsverträgen sollte daher ein Hinweis auf Reverse Engineering enthalten sein und ein solches Verhalten ausgeschlossen werden. Zusätzlich hat die Kommission im Erwägungsgrund 17 der Richtlinie zu bedenken gegeben, dass in Fällen parasitären Kopierens auch an eine Regelung über das UWG zu denken ist (Produktpiraterie oder sklavische Nachahmung). Vertragliche Beschränkungen sind aber regelmäßig zwecklos, wenn es gar keine Verträge gibt. Niemand kann einen Hersteller daran hindern, ein konkurrierendes Produkt auf dem freien Markt zu erwerben und im Wege des Austestens nachzubauen.

- 22 In Art. 3 Abs. 1 lit. c sind die Rechte des Betriebsrats geregelt, Informationen im Rahmen des sonstigen europäischen oder nationalen Rechts weiterzugeben. In Deutschland findet sich dazu eine Regelung in § 84 Betriebsverfassungsgesetz (BetrVG), der ein ausdrückliches Beschwerderecht des Arbeitnehmers bei Betriebsräten vorsieht. Die Richtlinie sieht allerdings in Erwägungsgrund 12 ausdrücklich vor, dass die Betriebsräte sich zur Verschwiegenheit mit dem Arbeitgeber verständigt haben können. § 79 BetrVG verpflichtet ohnehin die Mitglieder des Betriebsrates, Betriebsgeheimnisse nicht zu offenbaren und zu bewerten. Ähnliches sieht der § 99 Abs. 1 S. 3, § 102 Abs. 2 S. 5 BetrVG für personale Einzelmaßnahmen vor.
- 23 Art. 3 Abs. 1 lit. d erlaubt alle anderen Verhaltensweisen, die in Einklang mit seriösen Geschäftspraktiken stehen. Darin liegt eine Öffnungsklausel zugunsten der Judikative, in Anlehnung an die Fair-Use-Schranke im US-Recht. Erwägungsgrund 18 erwähnt als Beispiel die Offenlegung von Geschäftsgeheimnissen im Auditrecht.

## 2. Ausnahmen und Rechtfertigungsgründe (Art. 5)

- 24 Neu ist auch die Regelung der Ausnahmen in Art. 5 der Richtlinie. Zunächst werden die Unternehmen im Bereich der Presse- und der Informationsfreiheit freigestellt. Ausdrücklich wird verwiesen auf Art. 11 der Grundrechtecharta. Dadurch sind nicht nur Presseunternehmen im klassischen Sinne angesprochen, sondern eventuell auch Blogger.
- 25 In Art. 5 lit. b findet sich die zweite dem europäischen Recht noch fremde Institution, nämlich das Whistleblowing.<sup>38)</sup> Es ist definiert als das Offenlegen von Missständen oder illegalen Aktivitäten. Die Abgrenzung zwischen den beiden Tatbeständen ist unklar. Unklar ist auch, ob jeder kleine Rechtsverstoß als Legitimation für eine Offenlegung von Fehlverhalten ausreicht. Der Whistleblower kann sich nur auf die Schranke beziehen, wenn er im Interesse der Allgemeinheit gehandelt hat.<sup>39)</sup> Nicht eindeutig

ist, ob die Zweckbestimmung subjektiv oder objektiv zu verstehen ist. Erwägungsgrund 20 verweist auf ein Verhalten, das objektiv dem Allgemeininteresse dient. Außerdem nimmt die Präambel in Erwägungsgrund 20 auch ein Verhalten aus, das nach nationalstaatlichen Gerichtsurteilen als gutgläubig zu qualifizieren ist. Die Richtlinie deckt sich mit europäischen und nationalen Initiativen zur Verstärkung des Whistleblower-Schutzes. In Deutschland existierte lange Zeit allenfalls das Arbeitsschutzgesetz. Außerdem wurde in Einzelfällen § 34 StGB und die Anzeigepflichten nach § 138 StGB herangezogen. Ansonsten war die arbeitsrechtliche Rechtsprechung sehr restriktiv und verbot die Anzeige vor allem in der Öffentlichkeit vor Inanspruchnahme innerbetrieblicher Compliance-Systeme. So hat das Finanzdienstleistungsaufsichtsgesetz bereits zum 02.07.2016 Mitarbeiter der Finanzbranche von Verfolgung freigestellt, die gegenüber dem Bundesaufsichtsamt für das Versicherungswesen Missstände im Unternehmen anzeigen. Anders als nach bisherigem restriktiven deutschen Recht erlaubt die Richtlinie auch eine Offenlegung von Missständen in der Presse und ohne Beachtung einer innerbetrieblichen Abhilfe.<sup>40)</sup>

Die Beweislast für die Richtigkeit des Whistleblowing ist schwierig auszuloten. Der Ausnahmecharakter von Art. 5 der Richtlinie spricht dafür, dass der Whistleblower nachzuweisen hat, dass die Offenlegung der fraglichen Geschäftsgeheimnisse dem Schutz öffentlicher Interessen dient. Denkbar ist aber auch, dass das Unternehmen die Beweislast für die Richtigkeit oder Unrichtigkeit des Whistleblower trifft. Dieser Nachweis obliegt dem Unternehmen, während der Hinweisgeber nachweisen muss, dass er im öffentlichen Interesse handelte.

Art. 5 lit. c schließt die Kommunikation zwischen Arbeitnehmern und Betriebsrat weitestgehend vom Schutz von Geschäftsgeheimnissen aus. Eine Beschränkung auf Beschwerden oder die Mitteilung von Missständen wird nicht vorgenommen. Jedenfalls ist die gesamte Kommunikation ausgenommen, sofern diese für die Praxis der Betriebsräte notwendig ist.

Eine Generalklausel findet sich in Art. 5 lit. d, wonach jedes legitime Interesse eine Schranke rechtfertigt, das durch Unionsrecht oder nationales Recht erlaubt ist.

## VII. Sanktionen

Geregelt sind keine strafrechtlichen Sanktionen, da insofern keine Kompetenz der EU besteht. Vorgesehen ist vielmehr eine Pflicht der Mitgliedstaaten zur Einführung eines Sanktionssystems zivilrechtlicher Natur. Dies umfasst zahlreiche Rechtsfolgen, die bislang nur bei Monopolrechten gewährt wurden, und einen umfangreichen Schutz gegen rechtswidrigen Erwerb sowie gegen rechtswidrige Nutzung und Offenlegung der Geschäftsgeheimnisse. Umfasst sind Ansprüche auf Vernichtung oder Herausgabe der Dokumente, Gegenstände, Materialien, Stoffe oder elektronische Dateien, die das Geheimnis enthalten. Umfasst ist auch ein Rückrufanspruch rechtsverletzender Produkte und die Beseitigung und Vernichtung derselben. Ausführlich geregelt ist auch ein Schadensersatzanspruch. Allerdings fehlt ein bei anderen Schutzrechten vorgesehener Auskunftsanspruch (siehe § 140b PatG und § 242 BGB).

Zu klären ist jetzt durch das Justizministerium, inwiefern einzelne Sanktionen schon im deutschen Recht vorhanden sind. Die

38) Groß/Platzer, NZA 2017, 1097; Eufinger, ZRP 2016, 229.

39) Laposterle/Geiger/Olszak/Desaunettes, European Intellectual Property Review 255 (2016), Centre for International Property Studies (CEIPI) Research Paper No. 2015-02, S. 8 ff.

40) BAG, 07.12.2006 – 2 AZR 400/05, NZA 2007, 502; Umsetzung der Rechtsprechung des BVerfG, 02.07.2001 – 1 BvR 2049/00, NJW 2001, 3474 in der Entscheidung des BAG, 03.07.2003 – 2 AZR 235/02, NZA 2004, 427, 430; Ohly, GRUR 2014, 1, 7.

## Mallick/Weller, Aktuelle Entwicklungen im Influencer Marketing – Ein Blick aus der Praxis

Möglichkeit der dreifachen Schadensberechnung wird vom BGH<sup>41)</sup> zumindest für § 17 UWG anerkannt. Neu dürfte das System des Rückrufs und des Entfernens aus den Vertriebswegen sein.

- 31 Kompensatorisch zu diesem Strauß an Ansprüchen ist jetzt auch die Missbrauchskontrolle extensiv geregelt (Art. 7). Die Mitgliedstaaten müssen Möglichkeiten vorsehen, um den Beklagten vor missbräuchlichen Ansprüchen zu schützen. Diese Maßnahmen gehen über § 8 Abs. 4 UWG hinaus. Die Missbrauchssanktionen umfassen Schadensersatz für den Beklagten, Sanktionen gegen den Kläger oder die Verbreitung von Informationen über die abweisende Klage. Solche Maßnahmen sind derzeit in Deutschland unbekannt. Bekannt ist nur ein Schadensersatzanspruch bei unberechtigter Schutzrechtsverwarnung, d. h. bei Abmahnung aus besonderen gewerblichen Schutzrechten. Für das UWG ist allenfalls anerkannt, dass eine nachlässige Abmahnung ins Blaue hinein als unzulässiger Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb Schadensersatzansprüche begründen kann.<sup>42)</sup>
- 32 Die Rechtsbehelfsmaßnahmen umfassen vor allem die einstweilige Verfügung (Art. 12), gerichtet auf Unterlassung, Löschung und Verkaufsverbote. Statt der Unterlassung kommt auch ein verschuldensunabhängiger Anspruch auf Entschädigung (Lizenzanalogie) in Betracht (Art. 13 Abs. 3). Für den Schadensersatz (Art. 14) gilt die dreifache Schadensberechnung, einschließ-

lich entgangenen Gewinns, Verletzergevinns oder Lizenzanalogie. Besonders merkwürdig ist die Möglichkeit zur Erhöhung im Falle moralischer Schadensrisiken. Nicht gesehen wurde in der Richtlinie, dass zum Beispiel in Deutschland darüber hinausgehende Ansprüche aus §§ 812 und 687 Abs. 2 BGB entstehen können.<sup>43)</sup> Die Verjährungsfrist soll nicht mehr als sechs Jahre betragen.<sup>44)</sup>

## VIII. Fazit

Die Richtlinie wird das deutsche Geheimnisrecht nachhaltig ändern. Man kann daher gespannt sein auf die Umsetzung der Richtlinie 2018. Unternehmen sind dazu aufgefordert, schon jetzt konkrete Geheimhaltungsmaßnahmen vorzunehmen und sich auf das veränderte Umfeld von Geheimnissen einzustellen. Wichtig sind dabei vor allem erweiterte Geheimhaltungsvereinbarungen und eine Strategie zum Umgang mit der Freiheit von Reverse Engineering. Hinzu muss eine neue Kultur der Geheimhaltung in Unternehmen und mit Zulieferern kommen.

41) BGH, 18.02.1977 – I ZR 112/75, WRP 1977, 332, 335 – Prozeßrechner.

42) LG Hamburg, 08.05.2012 – 407 HKO 15/12, BeckRS 2012, 18887.

43) Weiterführend: Hauck, NJW 2016, 2218.

44) Nicht eingegangen werden soll auf die in der Richtlinie vorgenommenen Änderungen prozessualer Art, etwa in Korrektur des Düsseldorf Modells.

RAin Dr. Rani Mallick, Berlin und RA Dr. David Weller, Hamburg\*

## Aktuelle Entwicklungen im Influencer Marketing – Ein Blick aus der Praxis

### INHALT

- I. **Praktische Bedeutung von Influencer Marketing**
  1. **Wirtschaftliche Dimension**
  2. **Zielgruppe**
  3. **Verhältnis zwischen Influencer und Unternehmen**
- II. **Rechtsfragen des Influencer Marketings**
  1. **Rechtliche Grundlagen: RStV und TMG**
  2. **Die lauterkeitsrechtliche Betrachtung**
    - a) **Geschäftliche Handlung**
      - aa) **Unternehmen und Agenturen**
      - bb) **Influencer**
        - (1) **Influencer als Unternehmer**
        - (2) **Förderung des Absatzes eines fremden Unternehmens**
    - b) **Erkennbarkeit des kommerziellen Charakters**
      - aa) **Kennzeichnungsgewohnheiten in der Praxis**
      - bb) **Erkennbarkeit aus den Umständen?**
    - c) **Anforderungen an die Kennzeichnung**
    - d) **Sonstige Pflichten**
- III. **Fazit**

Influencer – darunter versteht man Persönlichkeiten, die über ihre Beiträge – so genannte Posts – in sozialen Medien wie Instagram und Facebook oder über Blogs einen großen Personenkreis erreichen, der weit über ihren tatsächlichen Bekanntenkreis hinausgeht. Dieser Personenkreis besteht aus sogenannten „Followern“, Personen, die die Beiträge des Influencers regelmäßig in ihren sozialen Netzwerken angezeigt bekommen oder dem Weblog eines Influencers folgen.

Wenden sich Influencer mit werblichen Botschaften an ihre Follower, ergeben sich rechtliche Probleme, die aktuell Wissenschaft, Gerichte und die anwaltliche Beratungspraxis beschäftigen. Der Beitrag von *Lehmann* in der WRP 7/2017 und der Beitrag von *Henning-Bodewig* in WRP 12/2017 setzen sich mit dem Phänomen des Influencer Marketing auseinander.<sup>1)</sup> Der vorliegende Beitrag nimmt die Praxis in den Fokus und versucht, alltagstaugliche Lösungen für die Frage der Einordnung eines Influencer Posts als geschäftliche Handlung und der ausreichenden Kennzeichnung zu entwickeln.

### I. Praktische Bedeutung von Influencer Marketing

Die Strahlkraft, die von Influencer Marketing ausgeht, beruht auf der viel gerühmten Authentizität und der Glaubwürdigkeit, die die Follower der Aussage eines Influencers beimessen. In Zeiten

\* Mehr über die Autoren erfahren Sie auf S. 259.

1) *Lehmann*, WRP 2017, 772 ff.; *Henning-Bodewig*, WRP 2017, 1415 ff.; vgl. auch das Editorial von *Lehmann*, WRP 06/2017.

## Wissenschaftsmeldung

Folgende Meldung wurde am 25.01.2018 um 11:20 an die VG WORT gesendet:

<b>Karteinummer:</b>	8801615
<b>Vorname:</b>	Thomas
<b>Nachname:</b>	Hoeren
<b>Geburtsdatum:</b>	22.08.1961
<b>Art des Werkes:</b>	Zeitschriften-Beitrag
<b>Name der Zeitschrift:</b>	Wettbewerb in Recht und Praxis
<b>ISSN:</b>	0508-6205
<b>Verlag:</b>	Dt. Fachverl.
<b>Verlagsort:</b>	Frankfurt, M.
<b>Erscheinungsjahr:</b>	2018
<b>1. Beitrag:</b>	
<b>Titel des Beitrags:</b>	Die EU-Richtlinie für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung
<b>Heftnummer:</b>	2
<b>Umfang in Normseiten:</b>	12
<b>Art der Beteiligung:</b>	Mit-Autor/in
<b>Anzahl der Autoren:</b>	2
<b>Weitere Autoren:</b>	Reiner Münker
<b>Verlagsbeteiligung:</b>	Sie haben einer Verlagsbeteiligung nicht zugestimmt.