8 | 2018

34. Jahrgang
15. August 2018
S. 485–552
PVSt 9892

CR

Computer und Recht

Zeitschrift für die Praxis des Rechts der Informationstechnologie

Schriftleitung: RA Prof. Dr. Michael Bartsch · RA Dr. Malte Grützmacher, LL.M. · RA Prof. Niko Härting · RA Sven-Erik Heun · RA Thomas Heymann · RA Prof. Dr. Jochen Schneider · RA Prof. Dr. Fabian Schuster · Prof. Dr. Indra Spiecker gen. Döhmann, LL.M. · Prof. Dr. Gerald Spindler

Herausgegeben gemeinsam mit DGRI e.V.

cr-online.de

Beratermodul CR

Mit CRi 4/2018

623

Frau Rechtsanwältin
Dr. Katharina Scheja
Elfelstr. 3
65812 Bad Soden

18187ZXCRX2018X8#1#107

Dr. Otto Schmidt KG - G.-Heinemann-Ufer 58 - 50968 Köln
PVSt, DPAG, Entgelt bezahlt, 09892

ottoschmidt

DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

CR Computer und Recht

Zeitschrift für die Praxis des Rechts der Informationstechnologie

IT und Software

Aufsätze

Katharina Scheja

Schutz von Algorithmen in Big Data Anwendungen

Wie Unternehmen aufgrund der Umsetzung der Geschäftsgeheimnis-Richtlinie ihre Algorithmen wie auch Datenbestände besser schützen können

Der Beitrag beschäftigt sich mit der Bedeutung und dem Schutz von Algorithmen (I.) und betrachtet aus dieser Perspektive die neue Geheimnisschutzgesetzgebung (II.). Vor diesem Hintergrund werden die Aufgaben zusammengefasst, die sich hierdurch für die juristische Beratungspraxis im Hinblick auf notwendige unternehmensinterne Vorkehrungen, Partner- und Arbeitnehmerverträge ergeben (III.).

I. Erst die Technik, dann das Recht

1 Die digitale Revolution ist bekanntlich in vollem Gange. Jedes Jahr verdoppelt sich die Menge an Daten, die die Menschheit erzeugt. Aktuelle Berechnungen gehen dahin, dass pro Jahr exponentiell mehr Daten erzeugt werden als in der gesamten Menschheitsgeschichte bis 2014 zusammengenommen.[1] Die Verarbeitung dieser gigantischen Datenmengen erfordert hochkomplexe Big Data Anwendungen und Analysen. Diese Anwendungen ihrerseits verlangen nach einer Vielzahl hoch komplizierter Algorithmen, die die Big Data Anwendung selbst ausmachen und die Auswertung dieser Daten auf alle erdenklichen Weisen ermöglichen. Die Erkennung von Schrift, Sprache, Bildern und Mustern durch Algorithmen hat ungeheure Fortschritte gemacht und schon jetzt werden z.B. mehr als 70 % aller Finanztransaktionen von Algorithmen gesteuert, nicht zuletzt alle Internet-User durch den Suchalgorithmus von *Google*. Algorithmen treiben auch die Entwicklung der künstlichen Intelligenz voran. So lernte etwa *Googles* Deep Mind Algorithmus autonom, 49 Atari Spiele zu gewinnen; weitere Beispiele sind zuhauf vorhanden. Kurz gefasst kann man Algorithmen als das Lebenselixier der digitalen Revolution ansehen.

Bisher stand diese ungeheure technologische und wirtschaftliche Bedeutung solcher als mathematischer Handlungsanweisung unscheinbar daherkommenden Ergebnisse menschlicher Erfindungstätigkeit im krassen Gegensatz zu ihrer Anerkennung als Schutzsubjekt der Rechtsordnung. Das Immaterialgüterschutzrecht, so muss man es wohl zusammenfassen, hat Algorithmen bisher einen effizienten Rechtsschutz versagt. Die *Europäische Union* hat mit ihrer 2016 erlassenen Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse; im Folgenden „Geschäftsgeheimnis-RL")[2] diese Schutzlücke geschlossen und damit aus hiesiger Sicht das Immaterialgüterrecht deutlich bereichert, indem sie für technologisches Know-how quasi eine neue Kategorie der Immaterialgüter einführt und neben Werke und Erfindungen stellt. Das ist ein großer Wurf, der das Immaterialgüterrecht für das digitale Zeitalter fit macht. Nun können 2

1 Https:www.spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen.

2 Geschäftsgeheimnis-RL (EU) 2016/943 vom 8.6.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtwidriger Nutzung und Offenlegung (Text von Bedeutung für den EWR) – http://data.europa.eu/eli/dir/2016/943/oj- nachfolgend kurz „Geschäftsgeheimnis-RL".

auch Schöpfungen der künstlichen Intelligenz, Geschäftsmethoden, allgemeines Know-how und eben Algorithmen[3] als solche eigenen Schutz erlangen; auch wenn insoweit keine Exklusivrechte begründet werden, ist dies im Hinblick auf die neuen Anspruchsgrundlagen und Rechtsverfolgungsmöglichkeiten eine kleine Revolution.[4]

3 Der deutsche Gesetzgeber hat nachgezogen und am 19.7.2018 den Regierungsentwurf für ein Geschäftsgeheimnisgesetz (GeschgG-RegE) vorgelegt[5], das die Geschäftsgeheimnis-RL in großen Teilen wortgleich und jedenfalls inhaltlich vollständig übernimmt. Der *Bundesrat* hat dem Gesetzentwurf zugestimmt, so dass insgesamt zu erwarten ist, dass der Entwurf im Herbst 2018 relativ rasch verabschiedet wird und Gesetzeskraft erlangt. Die Geschäftsgeheimnis-RL hatte den nationalen Gesetzgebern aufgegeben, den sich ergebenden Änderungsbedarf bis zum 9.6.2018 umzusetzen – seitdem findet sie nach den Voraussetzungen für eine unmittelbare Wirkung direkt Anwendung.[6] Damit ist den beteiligten Inhabern schon jetzt und künftig nach dem nationalen Geschäftsgeheimnisgesetz ein juristisches Instrumentarium an die Hand gegeben, Algorithmen für Big Data Anwendungen zu schützen und sicherzustellen, dass die Rechte an ihnen gesichert und verteidigt werden können. Dies erfordert allerdings zugleich eine Fülle an Umsetzungsmaßnahmen, die im Folgenden aufgezeigt werden.

II. Bedeutung und Schutz von Algorithmen

1. Was ist ein Algorithmus?

4 Ein Algorithmus hat zunächst einmal nicht unbedingt mit Computern zu tun. Es handelt sich um „nichts weiter" als eine definierte Abfolge von (Handlungs)schritten, die ein bestimmtes Ziel verfolgt. Schon bei der berühmten Handlungsanweisung an Aschenputtel „die Guten ins Töpfchen, die Schlechten ins Kröpfchen" oder – um es in das Büroleben fast vergangener Zeiten zu übertragen – „alle rote Briefe aus dem Posteingang zur Fakturierung und alle Blauen an den Einkauf" oder den sog. Body-Mass-Index – handelt es sich um nichts anderes als, allerdings einfache, Algorithmen. Kennzeichnend für Algorithmen sind eine Anzahl von sechs charakteristischen Eigenschaften:

- ▶ Eindeutigkeit,
- ▶ Ausführbarkeit,
- ▶ Finitheit (Endlichkeit),
- ▶ Terminierung,
- ▶ Determiniertheit und
- ▶ Determinismus.[7]

5 Computerprogramme und komplexe Big Data Anwendungen bestehen aus nichts anderem als einer Kette von Algorithmen. So wird die Börse schon lange vom Algorithmic-Trading bestimmt, also einem computer-gestützten Handel von Wertpapieren, bei dem der Computer nach mehr oder weniger komplexen Algorithmen in Millisekunden Wertpapiere kauft oder verkauft. Algorithmen werden in den Hydrauliksystemen von Bremsen eingesetzt (ABS) oder bei Paketdiensten zur Optimierung der Reihenfolge der Auslieferung. Algorithmen ermöglichen die Datenverarbeitung und Datenanalyse gigantischer Datenmengen ebenso wie die Entwicklung der künstlichen Intelligenz. Zugleich hat vorstehende Beispielliste für jeden, der mit dem Immaterialgüterschutz vertraut ist, bereits verdeutlicht, dass der Schutz von Algorithmen nach bisherigem deutschen Recht problematisch ist.

2. Schutz von Algorithmen nach bisher geltendem Recht

Nach bis dato geltendem deutschen Recht konnte man vor allem an folgende Rechtsgrundlagen denken, um den Schutz eines komplexen Algorithmus zu erreichen: Theoretisch in Erwägung zu ziehen waren (a) das Patentrecht, (b) das Urheberrecht und (c) der bisher im Gesetz gegen unlauteren Wettbewerb verankerte Schutz von Geschäftsgeheimnissen: 6

a) Patentrechtlicher Schutz von Algorithmen

Es wäre unrichtig festzustellen, dass Algorithmen *de lege lata* nicht patentrechtlich geschützt werden könnten. Dessen ungeachtet lässt sich aber festhalten, dass *in praxi* ein solcher Schutz in der Regel nicht zu erlangen oder dies jedenfalls auch nicht opportun war. Rechtlich problematisch ist die für eine Patentierbarkeit nach § 1 Abs. 1 PatG erforderliche Technizität. Im Standardkommentar zum Patentgesetz von *Benkard* findet sich folgende zusammenfassende Aussage: 7

„Algorithmen enthalten in der Regel Vorgaben, mit deren Hilfe nach den im Einzelnen festgelegten Regeln eine schrittweise Abwicklung von Arbeiten und Arbeitsvorgängen ermöglicht wird .... Ihr Ziel ist regelmäßig allein die Lösung von Problemen mit Mitteln der Logik; auf die Hilfe der Naturkräfte wird allenfalls bei ihrer tatsächlichen Umsetzung zurückgegriffen. Wie mathematische Methoden weisen Algorithmen, deren eher schematische Befolgung die Lösung gleichgelagerter Aufgaben 8

---

3 Die Geschäftsgeheimnis-RL erfasst neben „Know-how" auch sonstige Geschäftsgeheimnisse, wie z.B. Lieferanteninformationen. Der Aufbau der Auskunfts- und Schadensersatzansprüche ist aber eindeutig an das Konzept der Produktpiraterierichtlinie angelehnt – http://data.europa.eu/.... – wie sie dann in die entsprechenden Gesetze überführt wurde. Schadensersatz in der dem Immaterialgütterrecht bekannten dreifachen Berechnungsmöglichkeit unter Einschluss der Lizenzanalogie macht nur für lizenzierbare Schöpfungen Sinn, so dass man die Geschäftsgeheimnis-RL im Kern als auf technologisches Know-how zugeschnitten ansehen kann.

4 Anderer Auffassung insoweit *Koos*, „Die europäische Geschäftsgeheimnis-RL – ein gelungener Wurf?" MMR 2016, 224 ff.

5 Entwurf eines Gesetzes zur Umsetzung der Geschäftsgeheimnis-RL als Regierungsentwurf vorgelegt, nachfolgend „GeschgG-RegE". Siehe zum „geleakten" Referentenentwurf des Geschäftsgeheimnisgesetzes s. Aufsatz von *Lejeune*, „Das Geschäftsgeheimnisgesetz", ITRB 2018, 140 ff.

6 Die fehlende Umsetzung der Geschäftsgeheimnis-RL bis zum 9.6.2018 hat zur Folge, dass die Geschäftsgeheimnis-RL in Deutschland solange nach den Voraussetzungen der unmittelbaren Wirkung direkt anwendbar ist, bis sie in nationales Recht umgesetzt ist. Dies ist st. Rspr. des EuGHs, vgl. *Calliess/Ruffert/Ruffert*, 5. Aufl. 2016, AEUV Art. 288 Rz. 52 mit Verweis auf die EU-Rechtsprechung.

7 **Eindeutigkeit**: ein Algorithmus darf keine widersprüchliche Beschreibung haben; **Ausführbarkeit**: jeder einzelne Schritt muss ausführbar sein; **Endlichkeit**: die Beschreibung des Algorithmus muss endlich sein; **Terminierung**: nach endlich vielen Schritten muss der Algorithmus enden und ein Ergebnis liefern; **Determiniertheit**: der Algorithmus muss bei gleichen Voraussetzungen steht das gleiche Ergebnis liefern; **Determinismus**: zu jedem Zeitpunkt der Ausführung besteht höchstens eine Möglichkeit der Fortsetzung. Der Folgeschritt ist also eindeutig bestimmt.

ermöglicht .., unmittelbar nicht notwendig einen technischen Gehalt auf und sind daher insoweit nicht patentfähig..."[8]

9 In der Regel fraglich ist also der „*technische Gehalt*", was z.B. die Patentierbarkeit eines Algorithmus im Rahmen eines Antiblockiersystems ausgeschlossen hatte.[9] Grundsätzlich gilt, dass nicht schon der Algorithmus, sondern allenfalls seine Verwendung im Rahmen eines konkreten Programms Patentfähigkeit erlangen kann, wenn die dadurch aufgestellten Regeln den immer noch geforderten, „hinreichenden Bezug zur gezielten Anwendung von Naturkräften aufweisen". Bei dieser Ausgangslage wäre es riskant, einen Patentantrag einzureichen, da dies bekanntlich die umfassende Offenbarung der Erfindung, mithin des Algorithmus erfordert – der damit allseits bekannt werden würde. Schon dies dürfte in der Regel jedes Bemühen um einen patentrechtlichen Schutz *ad absurdum* führen – und selbst wenn dieser erreicht würde: über eine Patentierung kann sich mit Blick auf Algorithmen allenfalls ein auf die konkrete Verwendung in der jeweiligen Anwendung bezogener (zielgerichteter) Schutz ergeben[10]. Ein solcher Schutz schließt also grundsätzlich Dritte von einer Benutzung der gleichen Rechen- oder Handlungsregel im Kontext eines anderen Programms nicht aus, auch wenn dieses dem gleichen oder einem vergleichbaren Zweck dient.

b) Urheberrechtlicher Schutz

10 Das Urhebergesetz setzt insoweit die geltenden Rahmenbedingungen in § 2 und § 69a UrhG. Schon unter die Werkkategorien des § 2 Ziff. 1 UrhG sind einzelne Algorithmen nicht zu fassen, es sei denn man sieht ein Computerprogramm in seiner Gesamtheit als Algorithmus an.[11] Das scheint technisch fragwürdig; ein Computerprogramm besteht aus der Umsetzung von Algorithmen in Programmiersprache auf einen bestimmten Prozessor. Nun stellt § 69 Buchst. a) Ziff. 2 UrhG klar, dass auch alle Ausdrucksformen eines Computerprogramms geschützt sind, Ideen und Grundsätze jedoch nicht. Es ist daher mindestens fraglich, ob ein einzelner Algorithmus als mathematisch-logische Kette von Verarbeitungsanweisungen jenseits seiner konkreten Umsetzung in Programmiersprache wirklich ein Werk im Sinne des Urheberrechts sein kann – und zwar ungeachtet einer Schöpfungshöhe (so dass es auch nicht darauf ankäme, ob ein konkreter Algorithmus zum Standardrepertoire gehört oder nicht).[12] Anerkannt ist allerdings seit der Entscheidung des BGH „Betriebssystem", dass im Einzelfall *die konkrete Anwendung und Verknüpfung von Algorithmen* in einem Programm sowie *die Art und Weise ihrer Implementierung und Zuordnung zueinander* urheberschutzfähig sein können.[13] Wiewohl also ein urheberrechtlicher Schutz danach grundsätzlich für die Kombination von Algorithmen in einer Big Data Anwendung in Betracht kommt, ist jedenfalls fraglich, ob im Einzelfall die Voraussetzungen des Urheberrechts erfüllt werden können.[14]

c) Schutz als „Geschäftsgeheimnis"

11 Demgegenüber konnte schon auf Basis der bisherigen Gesetzeslage ein Schutz von Algorithmen als Geschäftsgeheimnis in Frage kommen. Durch die Verknüpfung der Strafnorm des § 17 UWG – Verrat von Geschäfts- und Betriebsgeheimnissen – mit §§ 823, 1004 BGB standen unter den dort genannten, allerdings engen Voraussetzungen auch zivilrechtliche Ansprüche u.a. auf Unterlassung und Schadensersatz zur Verfügung. Des Weiteren galt in der Rechtsprechungspraxis für Geschäftsgeheimnisse eine gewisse Privilegierung im Hinblick auf sonstige, aus anderen Gesetzen resultierenden Auskunfts- und Offenlegungsansprüchen. So hat der BGH eine „Score-Formel" – also einen Algorithmus zur Ermittlung von Wahrscheinlichkeitswerten für die Bonität einer Person – als Geschäftsgeheimnis von dem datenschutzrechtlichen Auskunftsanspruch eines Betroffenen ausgenommen.[15] Die klagende Betroffene hatte im Verfahren die Auffassung vertreten, dass es für sie nicht nachvollziehbar sei, wie einzelne Branchen-Scorewerte zustande gekommen seien; die Beklagte sei verpflichtet, die einzelnen Elemente, die in die Berechnung der Scores eingeflossen seien, offen zu legen. Der BGH hat diesen Anspruch mit der Begründung abgewiesen, dass zu den nach dem gesetzgeberischen Willen als Geschäftsgeheimnis geschützten Inhalten die Score Formel gehöre und damit im ersten Schritt die in die Score Formel eingeflossenen allgemeinen Rechengrößen, wie etwa die herangezogenen statistischen Werte, die Gewichtung einzelner Berechnungselemente bei der Ermittlung der Wahrscheinlichkeitswerte und die Bildung etwaiger Vergleichsgruppen als Grundlage der Scorekarten. Dies sei angesichts der aufwendigen Entwicklung des Score-Algorithmus, die spezielles Fachwissen voraussetze, auch nachvollziehbar und folgerichtig. Zudem hänge von dem Verfahren die Aussagekraft der Prognose und damit die Wettbewerbsfähigkeit sowie der Marktwert des Produkts und der Auskunftei selbst ab.[16] Im konkreten Fall konnte damit ein Auskunftsanspruch der Klägerin abgewehrt werden. Dessen ungeachtet konnte sich die Durchsetzung von Ansprüchen aufgrund einer missbräuchlichen Verwendung von Geschäftsgeheimnissen bislang als mühevolles bis aussichtsloses Unterfangen darstellen.

d) Neuerungen durch die Geschäftsgeheimnis-RL

12 Ohne an dieser Stelle eine detaillierte Gegenüberstellung der bisherigen Rechtslage mit der sich aus der Geschäftsgeheimnis-RL ergebenden Möglichkeiten durchzuführen, kann doch festgestellt werden, dass sich diese nunmehr erheblich verbessert

8 *Benkard*, PatG/Bacher, Anm. zu § 1 Rz. 98–98g in Kommentar zum Patentgesetz, 11. Aufl. 2015.

9 BGH v. 13.5.1980 – X ZB 19/78, GRUR 1980, 849, 850 – Antiblockiersystem.

10 *Benkard*, PatG/Bacher, a.a.O.

11 So insoweit OK-Kommentar Beck: BeckOK/UrhR/*Kaboth/Spies*, § 69a UrhG Rz. 12 „Algorithmen sind präzise Verarbeitungsvorschriften, die von einem mechanisch oder elektronisch arbeitenden Gerät durchgeführt werden können. Entsprechend ist jedes Computerprogramm in seiner Gesamtheit ein Algorithmus." Siehe auch *Dreier* in Dreier/Schulze, 5. Aufl. 2015, Kommentar zum UrhG, § 69a UrhG Rz. 22 mit weiteren Literaturhinweisen.

12 OK-Kommentar Beck: BeckOK/UrhR/*Kaboth/Spies*, § 69a UrhG Rz. 12 unter Verweis auf *Loewenheim* in Schricker/Loewenheim Rz. 12; *Dreier* in Dreier/Schulze § 69a UrhG Rz. 22.

13 BGH, GRUR 1991, GRUR Jahr 1991, Seite 449 – Betriebssystem.

14 Jedenfalls ist hierzu dem vorgenannten Urteil BGH „Betriebssystem" nicht zu entnehmen.

15 BGH, Urt. v. 28.1.2014 – VI ZR 156/13, CR 2014, 364 = BB 2014, 842 ff.

16 BGH, Urt. v. 28.1.2014 – VI ZR 156/13, CR 2014, 364 = BB 2014, 842, 844.

haben.[17] Der Geschäftsgeheimnis-RL kommt das Verdienst zu, die für die betroffenen Unternehmen schmerzlichen Schutzlücken zu schließen.[18]

13 Es fällt auf, dass die Geschäftsgeheimnis-RL schon in ihrem Titel den „know-how"-Schutz an die erste Stelle setzt. Die Intention der EU ist, durch die Geschäftsgeheimnis-RL ein eigenes Immaterialschutzrecht auf den Weg zu bringen, das weit über den bisherigen (strafrechtlichen) Geheimnisschutz des deutschen Rechts (wie auch anderer europäischer Rechtsordnungen) hinausgeht.

14 Diese Intention der EU wird in der Begründung an einer Vielzahl von Stellen deutlich: Gleich in Ziff. 1 der Erwägungsgründe wird auf den Schutz des Zugangs zu Wissen und die Verwertung von Wissen als Innovationsmotor abgestellt. Zwar gehe es bei Geschäftsgeheimnissen um ein breites Spektrum von Informationen, das über das technologische Wissen hinausgehend auch Geschäftsdaten wie Informationen über Kunden und Lieferanten, Geschäftspläne, Marktforschung und -strategien erfasst[19]; dem Richtliniengeber war es aber wichtig, gerade zum Schutze von kleinen und mittleren Unternehmen („KMU") wie auch innovationsstarken Unternehmen allgemein, eine breite Definition des Begriffs *„Geschäftsgeheimnis"* zu schaffen, die u.a. Geschäftsgeheimnisse und technologische Informationen umfassend abdeckt[20] und einen umfassenden zivilrechtlichen Schutz hierfür bereitzustellen. Dabei wird „Know-how" unter Verweis auf das „Übereinkommen über handelsbezogene Aspekte des geistigen Eigentums" (TRIPS) nunmehr ausdrücklich in den Schutzbereich des geistigen Eigentums aufgenommen.[21]

15 Konsequenterweise zieht die Geschäftsgeheimnis-RL entsprechende Parallelen, indem sie die im Immaterialgüterrecht bekannte Anspruchspalette von Auskunft, Beseitigung, Unterlassung, Vernichtung, Produktrückruf bis hin zur Urteilsveröffentlichung eröffnet und eine Schadensberechnung unter Anwendung der anerkannten Grundsätze der dreifachen Berechnung unter Einschluss der Lizenzanalogie (s. Art. 12 Geschäftsgeheimnis-RL und § 7 GeschgG-RegE) anregt[22]. Neben der Eröffnung des einstweiligen Rechtsschutzes einerseits wird andererseits im gerichtlichen Verfahren dem Interesse an der Aufrechterhaltung des Geheimnisschutzes durch eingeschränkte Zugangs- und Offenlegungsregelungen (s. Art. 9 ff. Geschäftsgeheimnis-RL) Rechnung getragen. Der GeschgG-RegE greift diese Vorgaben auf – wenn er sich auch nicht ausdrücklich für ein „in-camera"-Verfahren entscheidet – und übernimmt diese Regelungen in §§ 15 ff. GeschgG-RegE.

16 Aufgrund der Geschäftsgeheimnis-RL und deren nationaler Umsetzung kann ein Algorithmus, der als Geschäftsgeheimnis anzusehen ist, nunmehr wie eine Erfindung oder ein Computerprogramm geschützt, lizenziert und weitergegeben werden. Dieses Zwischenergebnis ist erfreulich, aber wie immer gilt, dass die Inanspruchnahme dieser Möglichkeiten nicht ohne Anstrengung zu erlangen ist.

e) Neue Anforderungen für „Geschäftsgeheimnisse"

17 Denn die Geschäftsgeheimnis-RL stellt – neue – Anforderungen auf, die an ein Geschäftsgeheimnis zu stellen sind. Als Geschäftsgeheimnis ist eine Information nur dann geschützt, wenn sie eine Reihe von Kriterien erfüllt. Die Information muss nach Art. 2, Ziff. 1, Buchstaben a) – c) der Geschäftsgeheimnis-RL

(i) *„geheim"* sein,

(ii) deswegen einen *„kommerziellen Wert"* haben und

(iii) des Weiteren müssen *„angemessene Geheimhaltungsmaßnahmen"* getroffen werden.

18 Das deutsche Recht knüpfte bisher an einen Geheimhaltungswillen an, was konkrete angemessene Geheimhaltungsmaßnahmen nicht erforderte[23]; der GeschgG-RegE greift die neue Anforderung der Geschäftsgeheimnis-RL inhaltsgleich in § 1 Ziff. 1 und 2 auf. Die Verwertung des Geschäftsgeheimnisses steht dem Inhaber zu; das ist gem. Art. 2, Ziff. 2 Geschäftsgeheimnis-RL und § 1 GeschgG-RegE jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis besitzt. Die nachfolgenden Ausführungen sollen die sich hieraus für Unternehmen ergebenden Handlungsanforderungen beleuchten.

III. Konsequenzen für die Rechtspraxis

19 Unternehmen, die auf Basis dieser neuen gesetzgeberischen Situation ihre Rechte an technologischen Erfindungen und Entwicklungen und insbesondere Algorithmen schützen wollen, müssen daher an verschiedenen Stellen aktiv werden. Sie müssen in einem ersten Schritt ihre Inhaberschaft sichern, sich also durch vertragliche Vereinbarungen mit ihren Mitarbeitern und Dienstleistern die Rechte an Geschäftsgeheimnissen sichern und ihre Benutzung und Offenlegung regeln (dazu 1.). Des Weiteren müssen sie technische und organisatorische Maßnahmen treffen, um Geschäftsgeheimnisse angemessen zu schützen (dazu 2.). Last but not least müssen sie in ihren Vereinbarungen mit Geschäftspartnern entsprechend auf die neuen gesetzlichen Bestimmungen abgestellte vertragliche Regelungen treffen (dazu 3.).

1. Sicherung der Inhaberschaft

a) Ausübung der Kontrolle zur Erlangung der Inhaberschaft

2 Nach der Legaldefinition von Art. 2 Ziff. 2 Geschäftsgeheimnis-RL und gleichlautend § 1 Abs. 1 Ziff. 2 GeschgG-RegE ist Inhaber eines Geschäftsgeheimnisses „jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Ge-

17 Siehe *Kalbfus*, „Die EU-Geschäftsgeheimnis-Richtlinie", GRUR 2016, 1009 ff.; *Heinzke*, Richtlinie zum Schutz von Geschäftsgeheimnissen", CCZ 2016, 179 ff.; *Koos*, „Die europäische Geschäftsgeheimnis-Richtlinie – ein gelungener Wurf?" MMR 2016, 224 ff.

18 Die Kritik an der Intransparenz von algorithmus-gesteuerten, automatisierten Entscheidungsprozessen ist eine politische Diskussion und steht hier – so wichtig sie ist – nicht im Fokus; ein Gleiches gilt für die Diskussion um „whistle-blowing" und die Kritik an der Geschäftsgeheimnis-RL, dass dies whistleblower nicht schütze.

19 EU-Geschäftsgeheimnis-RL, a.a.O., Ziff. 2, RiLi-Begründung.

20 EU-Geschäftsgeheimnis-RL, a.a.O., Ziff. 10, 14 und 16 Ri-Li Begründung.

21 EU-Geschäftsgeheimnis-RL, a.a.O., Ziff. 4, 5, 6 und 7 Ri-Li Begründung.

22 Siehe hierzu konkret: *Böhm/Nestler*, „EU-Richtlinie zum Know-how-Schutz: Quantifizierung des Schadensersatzes", GRUR-Prax. 2018, 181 ff.

23 Siehe hierzu *Kalbfus*, a.a.O.

schäftsgeheimnis besitzt". Wer die Inhaberschaft an einem Geschäftsgeheimnis für sich reklamieren will, muss sich in einem *ersten Schritt* also die rechtmäßige Kontrolle über das Geschäftsgeheimnis sichern. Dazu bedarf es vertraglicher Regelungen – mit den das Geschäftsgeheimnis Schaffenden wie anderen Beteiligten. An dieser Stelle sei ein Exkurs zu dem seit einiger Zeit heftig diskutierten Thema des „Eigentums an Daten" erlaubt[24]. Ein einzelnes Datum kann – ebenfalls wie eine mithilfe von Algorithmen aufbereitete und analysierte Datensammlungen – nach der breiten Definition ein technologisches Geschäftsgeheimnis sein. Die heiß diskutierte Frage, wem solche Geschäftsgeheimnis-Daten gehören, beantwortet sich mit der Geschäftsgeheimnis-RL *de lege lata* dahingehend, dass dies ihr Inhaber im Sinne vorgenannter Definition ist. Verfolgt man den bereits anhängigen Streit in der Industrie – etwa zum Streit zwischen *Lufthansa* einerseits und *Airbus* sowie *Boing* andererseits um Flugzeugdaten[25] – stellt man rasch fest, dass der Streit um den Besitz der Kontrolle dieser ebenso wertvollen wie sensiblen Geschäftsgeheimisse bereits im vollen Gange ist. Die Airlines müssen befürchten, Zugriff und Kontrolle über die in den Flugzeug(gerät)en gesammelten Daten durch Verschlüsselung und Zugriffssperren seitens der Flugzeug-Hersteller zu verlieren. Tatsächlich dürfte die tatsächliche Kontrolle über diese Daten bei den Flugzeugherstellern liegen, diese damit als „Inhaber" im Sinne der Geschäftsgeheimnis-RL gelten und daher insoweit privilegiert sein. Die einzige Möglichkeit, diese Rechtsposition zugunsten anderer Marktbeteiligter zu verändern, besteht in entsprechenden vertraglichen Regelungen, die die Kontrolle und den Besitz von Datenbeständen und Geschäftsgeheimnissen angemessen aufteilen.[26]

b) Überarbeitungsbedürftige Klauseln in Beschäftigungsverträgen

21 Inhaber eines Geschäftsgeheimnisses kann zunächst jede natürliche oder juristische Person sein. Danach ist es nicht unbedingt erforderlich, dass ein geschäftlicher Betrieb geführt wird. Auch dies verdeutlicht wiederum, dass die Geschäftsgeheimnis-RL in ihrem Schwerpunkt technologisches Know-how schützt, denn solches kann durchaus auch eine Privatperson geschaffen haben, die damit „Inhaber" ist und entsprechend wie ein Erfinder anspruchsberechtigt und im Prozess aktivlegitimiert ist. Anders als in § 17 UWG wird hier nicht das Unternehmen und der Geschäftsinhaber privilegiert, sondern grundsätzlich jeder Know-how Schaffende.

22 Diese weitere Feststellung zur Inhaberschaft ist wichtig, denn Geschäftsgeheimnis-RL und GeschgG-RegE beinhalten keine dem § 69b UrhG (Urheber in Arbeits-oder Dienstverhältnissen) oder § 1 ff. Arbeitnehmererfindungsgesetz entsprechende Bestimmung, die die Arbeitsergebnisse von Arbeitnehmern regelmäßig in die Herrschaftsmacht des Arbeitgebers übergeben. Da es sich bei der Entwicklung von Algorithmen oder speziellen Mechanismen für Big Data Anwendungen weder um patent- noch gebrauchsmusterfähige Erfindungen i.S.v. § 2 ArbeitnehmererfindungsG handelt (s. II.2.a) Rz. 7-8 oben), noch regelmäßig um urheberrechtsschutzfähige Werke, kommt eine Beanspruchung des Arbeitgebers nach diesen Regelungen nicht zur Anwendung. Es ist daher in Arbeits-, Dienst- und Werkverträgen zukünftig besonderes Augenmerk darauf zu richten, dass auch hinsichtlich von Geschäftsgeheimnissen und Know-how, an dessen Erstellung der Arbeitnehmer oder Vertragspartner beteiligt ist, dem Tätigkeit- und Einsatzbereich entsprechende Rechtseinräumungsklauseln aufgenommen werden. Zu vermeiden ist dabei andererseits, über das Ziel hinaus zu schießen.

Dem Vertragspartner darf – auch im Arbeitsverhältnis – schon 23
aus Gründen der Berufsfreiheit nicht versagt werden, seine Fähigkeiten und Kenntnisse auch nach Beendigung des Arbeitsverhältnisses einzusetzen; aus dem Anwendungsbereich des Begriffs Geschäftsgeheimnis fallen nach der ausdrücklichen Regelung der Geschäftsgeheimnis-RL belanglose Informationen und Erfahrungen und Qualifikationen, die Beschäftigte im Zuge der Ausübung ihrer üblichen Tätigkeit erwerben.[27] In Anlehnung an die Bestimmungen z.B. des Urheberrechts ist es jedoch legitim, wenn der Geschäftsinhaber die wesentlichen Vorarbeiten und Arbeitsergebnisse reklamiert, die ein Know-how oder Geschäftsgeheimnis-Schaffender in Erfüllung seiner vertraglichen Verpflichtungen erstellt oder mit erarbeitet hat. In einem *zweiten Schritt* ist daher eine Überprüfung aller Arbeits- und Dienstverträge und der dort enthaltenen Tätigkeitsbeschreibung zu empfehlen; diese Beschreibung der geschuldeten Aufgaben und Pflichten sollte gerade im Bereich von Forschungs- und Entwicklungsabteilungen mit der nötigen Sorgfalt vorgenommen werden.

b) Zuordnung der Arbeitsergebnisse

In einem *weiteren Schritt* ist es erforderlich, dass diese Arbeits- 24
ergebnisse auch zweifelfrei bestimmbar sind. Die Definition des Inhabers als demjenigen, der die (rechtmäßige) Kontrolle ausübt, macht dies implizit zu einer weiteren Anforderung der Inhaberschaft. Wer keine Kontrolle hat, kann auch nicht Inhaber eines Geschäftsgeheimnisses sein. Auch aus diesem Grund ist die genaue vertragliche und tatsächliche Festlegung von Geschäftsgeheimnissen essenziell. Im Programmierbereich sind z.B. Datenbanken üblich, in denen die Entwickler die zugewiesenen Aufgaben, ihren Erledigungsstatus und die Arbeitsergebnisse hinterlegen. Dies sollte Standard in allen Forschungs- und Entwicklungsabteilungen sein, denn nur so kann der Gegenstand einer Rechtseinräumung *eindeutig* bestimmt werden und der sonst schwierige Nachweis geführt werden, „was" ein Arbeitnehmer geschaffen hat und ob dies auch „in Erfüllung vertraglicher Pflichten"[28] oder „aus der dem Arbeitnehmer im Betrieb obliegenden Tätigkeit" geschaffen wurde.[29] Jedwede Rechtseinräumung läuft ins Leere, wenn der Schutzgegenstand nicht eindeutig bestimmt werden kann und seine Zuordnung

24 Siehe zuletzt und richtungsweisend: *Thomas Heymann*, „Rechte an Daten – warum Daten keiner eigentumsrechtliche Logik folgen", CR 2016, 650 – 657 mit weiteren Nachweisen.

25 Siehe hierzu „Die Welt Kompakt" vom Dienstag, 24.7.2018, S. 26/27.

26 Wie ausgeführt, wird durch die Geschäftsgeheimnis-RL eine immaterialgüterschutzähnliche Rechtsposition vermittelt, aber keine Exklusivrechte; die zur Ausübung dieser Position erforderliche Verteilung der Rechte hieran durch Verträge vermeidet richtigerweise sowohl die ungerechtfertigte Verleihung eigentümerähnlicher Absolutheitsrechte als auch die Missachtung anderer, gesetzlichen schützenswerter Interessen.

27 So auch ausdrücklich die Geschäftsgeheimnis-RL in Ziff. 14 am Ende der Erwägungsgründe der Geschäftsgeheimnis-RL.

28 So die Formulierung in § 69b UrhG.

29 So § 4 Abs. 2 ArbeitnehmererfindungsG.

zum vertraglichen Pflichtenkreis nicht einwandfrei feststellbar ist.

2. Geschäftsgeheimnis

a) Wirtschaftlicher Wert und Zugänglichkeit

25 Nach der Definition in Art. 2 Ziff. 1 Geheinmis-RL und § 1 Abs. 1 Ziff. 1 a) GeschgG-RegE muss ein Geschäftsgeheimnis zunächst in dem Sinne geheim sein, dass es weder „in der Gesamtheit 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 ist und daher von wirtschaftlichem Wert ist".[30]

26 Dass ein Geschäftsgeheimnis nicht allgemein bekannt sein darf, war auch schon bisher eine – soweit ersichtlich – universelle Anforderung diverser Rechtsordnungen. Man könnte allerdings in der Formulierung „nicht ohne weiteres zugänglich" jedenfalls für den Bereich technologischen Know-hows das Erfordernis einer gewissen „Schöpfungshöhe" hineinlesen. So hat bereits der BGH in der Entscheidung „Score-Formel"[31] an die „aufwendige Entwicklung des Score-Algorithmus, die spezielles Fachwissen voraussetze" angeknüpft. Sollte diese Rechtsprechungslinie in Zukunft fortgeschrieben werden, könnten lediglich triviale Algorithmen richtigerweise – wenn nicht allgemein bekannt – so doch als „ohne weiteres zugänglich" im Sinne von: ohne weiteres „herstellbar" – aus dem künftigen Schutzbereich des Geschäftsgeheimnisgesetzes herausfallen, weil ihre Entwicklung eben kein besonderes Fachwissen voraussetzt. Eine solche einschränkende Auslegung wäre ein weiterer Schritt in Richtung einer Angleichung an allgemein immaterialgüterschutzrechtliche Grundsätze.

b) Angemessenheit von Geheimhaltungsmaßnahmen

27 Hinsichtlich dieser objektiven Anforderungen ist ansonsten über das unter 1. Rz. 20 oben beschriebene Tätigkeitsprogramm hinaus nichts zu unternehmen.

28 Neuland beschreitet der deutsche Gesetzgeber bei der unter Art. 2, Ziff. 1, Buchst c) der Geschäftsgeheimnis-RL/§ 1 Abs. 1 Ziff. 1 b) GeschgG-RegE statuierten weiteren Voraussetzung „angemessener Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber": Danach reicht es für den Geschäftsinhaber *erstens* nicht, wenn er die Geheimhaltung seinen Angestellten überlässt, denn nach dem Wortlaut des Gesetzestextes obliegt diese Verpflichtung dem, der ein Geschäftsgeheimnis für sich beanspruchen will. *Zweitens* sind explizit nunmehr Geheimhaltungsmaßnahmen erforderlich.

29 Zur Frage allerdings, was insoweit „angemessene" Maßnahmen sein könnten, schweigt sich die Geschäftsgeheimnis-RL ebenso aus wie der GeschgG-RegE. Unbekannt ist dieser Begriff hingegen nicht; er hat seinen Ursprung vermutlich in den USA und findet sich in den Gesetzen anderer Länder wie auch TRIPS[32] erwähnt. Allerdings ist insofern keine Rechtsprechung ersichtlich, auf die zur Konkretisierung dieser neuen Anforderung Bezug genommen werden könnte. Es macht auch jedenfalls Sinn, den im deutschen Recht bisher geforderten, subjektiv angelegten Geheimhaltungswillen durch einen objektiven Maßstab zu ersetzen.[33]

c) Neuer Anwendungsbereich für „Technisch-Organisatorische Maßnahmen"

Vor diesem Hintergrund scheint es nicht verfehlt, für den 30
Schutz von Geschäftsgeheimnissen auf die Standards zurückzugreifen, die in anderen Rechtsbereichen seit langem Geltung haben. Zu denken wäre hier z.B. an geheimnisschutzspezifische TOMs – also spezielle technisch-organisatorische Maßnahmen – zum Geschäftsgeheimnisschutz im Unternehmen. Damit würde sich im übrigen für das sicherheitsrechtliche Pflichtenprogramm von Unternehmen ein Kreis schließen, der von dem sich entwickelnden Schutzkonzept im Bereich der IT Sicherheit[34] bis hin zum Schutz persönlicher Daten nun auch die Geschäftsgeheimnisse erfasst. Die sich stellende Aufgabe ist es, auch für diesen Bereich einen speziellen Maßnahmenkatalog zu definieren, der den Schutz von Geschäftsgeheimnissen in den Blick nimmt. Dabei sollten vier Eckpunkte in Erwägung gezogen werden und mit dem bestehenden IT-Sicherheitskonzept und TOMs abgeglichen werden:

i. *Einordnung von Geschäftsgeheimnissen in Schutzklassen* 31

Dieses – nicht von ungefähr aus dem militärischen Bereich – resultierende Vorgehen der Einteilung in Schutzklassen wie „Vertraulich" – „Geheim" – „Hochgeheim" ist der erste Schritt, um ein der Wichtigkeit und Bedeutung der jeweiligen Geschäftsgeheimnisse „angemessenes" Schutzsystem zu implementieren.[35] Hierzu sollten zunächst im Unternehmen die verschiedenen Bereiche an Geschäftsgeheimnissen identifiziert werden; es sollte auch ganz bewusst darüber nachgedacht werden, für welche Kategorien von Geschäftsgeheimnissen Schutzmaßnahmen besonderer Art sinnvoll sind. Richtigerweise wären die zentralen Arbeitsergebnisse der Forschungs- und Entwicklungsabteilung ebenso in die Klasse „Hochvertraulich" einzuordnen wie die Protokolle von Vorstandssitzungen. Auch hier gilt aber wie überall, dass eine inflationäre Einstufung in die Hochvertraulich-Kategorie kontraproduktiv ist. Außerdem wäre es sinnvoll, soweit als möglich einen Gleichlauf mit den Maßnahmen in anderen Bereichen (etwa den datenschutzrechtlichen TOMs) zu erreichen (wo auch zwischen „einfachen" und „besonders sensitiven" personenbezogenen Daten zu unterscheiden ist).

---

30 Die Formulierung in § 1 Ziff. 1 a) des GeschgG-RegEs weicht an dieser Stelle geringfügig vom Text der Geschäftsgeheimnis-RL ab.

31 Siehe BGH, BB 2014, Seite 840.

32 Siehe hierzu *Kalbfus*, „Angemessene Geheimhaltungsmaßnahmen nach der Geschäftsgeheimnis-Richtlinie", GRUR-Prax. 2017, 391, 392, mit weiteren Nachweisen.

33 Siehe hierzu *Kalbfus*, a.a.O: „Angemessene Geheimhaltungsmaßnahmen ...", 392.

34 Siehe *Frisse/Glassl/Baranowski/Duwald*, „Unternehmenssicherheit bei Banken – IT-Sicherheit, Know-how-Schutz, Datensicherheit und Datenschutz", BKR 2018, 177 ff. (speziell für den Bankensektor); *Kipker*, „Die NIS-RL der EU im Vergleich zum deutschen IT-Sicherheitsgesetz", ZD-Aktuell 2016, 05261 ff. *Schreibhauer/Spittka*, IT-Sicherheitsgesetz: neue Anforderungen für Unternehmen", ITRB 2015, 240 ff.; *Hornung*, „Neue Pflichten für Betreiber kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes", NJW 2015, 3334 ff.

35 So auch *Kalbfus*, „Angemessene Geheimhaltungsmaßnahmen ...", a.a.O., 393 f.

32 **ii.** *Vorgaben für Zugangs-, Zugriff und Veränderungsberechtigungen*

In diesem Bereich kann relativ weitgehend auf übliche Regelungen in datenschutzrechtlichen TOM-Vorlagen zurückgegriffen werden. Es wird hierbei gehen einerseits um die physische Zugangskontrolle, die ein ständiges Monitoring von zugangsbeschränkten Bürobereichen durch Kameras und/oder Schutztüren, Wachdienst oder eine Kombination aus all diesen vorsehen sollte. Andererseits ist genauso erforderlich – wenn nicht noch wichtiger – dass der Zugriff auf IT-Systeme genau geregelt und überwacht wird. Es müssen Maßnahmen getroffen werden zur Zugangskontrolle durch Schlüssel- und Passwörtern, Vorgaben, wie diese zu schützen und regelmäßig zu ändern sind, Zugang- und Veränderungsregelungen für bestimmte Dokumente und Dokumentenklassen und Server sowie Systeme, bis hin zu Vorgaben hinsichtlich der Speicherung, Weiterleitung und des Kopierens. Jedes Unternehmen sollte insofern bereits Anweisungen im Hinblick auf Datenschutz und IT Sicherheit haben, auf die unter dem Aspekt des Geschäftsgeheimnisschutzes ein prüfender Blick geworfen werden sollte.

33 **iii.** *Besondere Sicherheitsmaßnahmen für (hochsicherheitsrelevante) Geheimnisse*

Die Sicherheitsarchitektur von IT-Systemen wird mittlerweise in großem Maße von gesetzgeberischen Vorgaben und in Zusammenhang damit stehenden ISO-Normen und anderen Standards bestimmt.[36] Unternehmen, die diese Maßnahmen sorgsam umsetzen, kontinuierlich überprüfen und aktualisieren, sollten insoweit *de jure* das Erforderliche getan haben, um auch für ihre Geschäftsgeheimnisse „angemessene Schutzmaßnahmen" dokumentieren zu können. Es wäre aber in Erwägung zu ziehen, und wird vereinzelt auch praktiziert, bestimmte Arbeitsgruppen in der F&E-Abteilung mit ihren Arbeiten und Entwicklungsergebnissen insgesamt aus den allgemeinen IT Systemen und dem Internet (!) abzukoppeln, um autarke und isolierte Arbeitsgruppen für hochsensible Geschäftsgeheimnisquellen zu schaffen, innerhalb derer isoliert und sicher kommuniziert, gearbeitet und gespeichert werden kann. Der Ausschluss externer Speicherungsmittel (USB Stick, DVD und alles Weitere) von solchen getrennten IT-Systemen versteht sich in einem solchen Hochsicherheitstrakt ebenso wie vorinstallierte Bildschirmschoner, die das Abfotografieren unterbinden. Die Hinzuziehung professioneller Sicherheitsexperten aus dem Bereich der Spionageabwehr ist hierbei durchaus nicht unüblich. Derzeit würde es sich dabei um Maßnahmen handeln, die ein Unternehmen im eigenen Interesse initiiert, weil nicht erkennbar ist, ob die Rechtsprechung unter den Oberbegriff „angemessene" Schutzvorkehrungen so weitgehende Abschirmung verlangen würde.

34 **iv.** *Überprüfung, Beurteilung und Evaluation der Maßnahmen*

Die Wirksamkeit der getroffenen Maßnahmen, auch die im Bereich der IT Sicherheit üblichen Penetrationstests, sollten das Portfolio der Schutzmaßnahmen auch für Geschäftsgeheimnisse abrunden.

35 Zusammenfassend würde es sich also anbieten, zunächst die vorhandenen Geschäftsgeheimnisse in Schutzklassen einzuteilen. Sodann könnte man auf die bereits bestehenden IT- und sonstigen Sicherheitsvorgaben zurückgreifen sowie die aufgrund datenschutzrechtlicher Vorgaben erarbeiteten technisch-organisatorischen Maßnahmenkataloge. Diese sollten abgestuft nach den vorgenannten Schutzklassen dann auch für Geschäftsgeheimnisse herangezogen bzw. vereinbart und gegebenenfalls um weitere oder andere Maßnahmen ergänzt werden. In diesem Zusammenhang wäre auch zu überlegen, ob nicht neben dem Datenschutzbeauftragten und den gegebenenfalls bereits vorhandenen IT-Sicherheitsbeauftragten auch ein Mitarbeiter mit der Kontrolle und Überwachung des Schutzes von Geschäftsgeheimnissen betraut werden sollte.

3. Überarbeitungsbedürftige Klauseln in Partnerverträgen

36 Nach diesen Vorarbeiten zur Sicherung der Inhaberschaft wie der Bestimmbarkeit eines Geschäftsgeheimnisses wäre im letzten Schritt dem Schutz von Geschäftsgeheimnissen in solchen Verträgen mit Geschäftspartnern Rechnung zu tragen, bei denen Geschäftsgeheimnisse durch Offenbarung, Austausch oder Lizenzierung oder auch angelegentlich der Vertragsbeziehung tangiert werden. Wie vorstehend ausgeführt, ist hier auch an z.B. Flugzeugkaufverträge zu denken; soweit es sich bei den tangierten Geschäftsgeheimnissen um Daten oder Datensammlungen oder Algorithmen handelt, sind Regelungen über Besitz und Kontrolle unabdingbar. Allseits bekannt sind in Verträgen aller Art die üblichen Geheimhaltungsklauseln. Diese dienen dem Schutz allgemein vertraulicher Informationen und sind nicht speziell auf Know-how zugeschnitten. Gleiches gilt für „non-disclosure-agreements", die im Bereich patentfähigen Know-hows schon lange üblich sind. Es ist die Auffassung der Verfasserin, dass diese Klauseln einer umfassenden Neubeurteilung und Umformulierung unterliegen sollten. Es ist z.B. zu beachten, dass die Geschäftsgeheimnis-RL das „reverse engineering" von Know-how im Interesse der Innovationsförderung als rechtlich zulässiges Mittel zum Erwerb von Informationen ansieht – es sei denn, dass vertraglich etwas anderes vereinbart wurde.[37] In Rechtseinräumungsklauseln sollte daher auch der Verteilung der Rechte an Know-how und Geschäftsgeheimnissen größeres Augenmerk gewidmet werden. Einer Überprüfung zu unterziehen wären:

i. *Alle Verträge*, die in irgendeiner Form mit Geschäftsgeheimnissen zu tun haben – also auch z.B. Kaufverträge über Maschinen, die Datensammelcomputer und/oder Big-Data-Anwendungen eingebaut haben.[38]

ii. *Vertraulichkeitsklauseln* im Hinblick auf die Weitergabe der Verpflichtung zu angemessenen Schutzvorkehrungen sowie im Einzelfall erforderliche Offenlegungsvoraussetzungen

36 Siehe hierzu mit weiterführenden Hinweisen: *Gitter/Meißner/Spauschus*, „Das neue IT-Sicherheitsgesetz – IT-Sicherheit zwischen Digitaliserung und digitaler Abhängigkeit", ZD 2015, 512 ff.; s. insbesondere auch ISO 27001-Zertifizierung sowie IT-Grundschutzkatalog des BSI – Bundesamtes für Sicherheit in der Informationstechnologie.

37 Siehe Ziff. 16 und 17 der Erwägungsgründe der Geschäftsgeheimnis-RL.

38 Im Hinblick auf die Internet-of-Things Diskussion eminent wichtig.

iii. *Rechtseinräumungsklauseln* im Hinblick auf spezielle Regelungen zur Lizenzierung und weiteren Benutzung von Know-how und Geschäftsgeheimnissen sowie gegebenenfalls Ausschluss von Reverse Engineering Maßnahmen

iv. *Rechtsverfolgungsklauseln*, die die Aufgabenverteilung im Fall von Ansprüchen gegen Dritte regeln

v. *Freistellungsklauseln*, die den internen Schadensausgleich regeln.

IV. Fazit und Ausblick

37 Das auf Vorgabe der Geschäftsgeheimnis-RL alsbald Inkrafttretende Geschäftsgeheimnisgesetz wird eine umfassende Neuordnung des Schutzes insbesondere von technologischem Know-how und damit auch von Algorithmen zur Folge haben. Es ist wichtig, die sich hieraus ergebenden Möglichkeiten in den Blick zu nehmen und den sich daraus ergebenden Aufgabenkatalog zu bestimmen und abzuarbeiten. Für Unternehmen stellen sich in diesem Zusammenhang eine Reihe von Aufgaben:

38 Wichtig ist zunächst eine *Überprüfung der Standardverträge mit Dienstleistern und Arbeitnehmern* im Hinblick auf die Rechtseinräumung an Know-how und den Schutz vertraulicher Informationen. Des Weiteren muss das in einem Unternehmen erarbeitete und eingesetzte Know-how „gerichtsfest" *bestimmbar gemacht* gemacht werden. Hierzu ist in der täglichen Praxis sicherzustellen, dass Entwicklungsergebnisse dokumentiert, gespeichert und archiviert werden und jederzeit bestimmten Personen zugeordnet werden kann. Der Geschäftsinhaber muss Kontrolle ausüben können, was die Bestimmbarkeit der Geschäftsgeheimnisse voraussetzt.

39 Des Weiteren ist es erforderlich, durch die Erarbeitung von *technisch organisatorischen Maßnahmenkatalogen* „angemessene Schutzmaßnahmen" im Unternehmen zu bestimmen. Hier wäre an die Einteilung von Geschäftsgeheimnissen in Schutzklassen und hierauf abgestimmte Schutzmaßnahmen zu denken. Hinsichtlich von Schutzmaßnahmen kann ganz weitgehend auf in anderen Bereichen erarbeitete technische-und organisatorischen Maßnahmenkataloge – z.B. aus dem Bereich Datenschutz und IT-Sicherheit – zugegriffen werden, die allerdings hinsichtlich der Besonderheiten von Geschäftsgeheimnissen gegebenenfalls überarbeitet, ergänzt und überprüft werden müssen. Es wäre bedenkenswert, gegebenenfalls einen Sicherheitsbeauftragten für Geschäftsgeheimnisse zu etablieren, der die Kontrolle über die Einhaltung der Maßnahmen und ihre Aktualisierung ausübt.

Schließlich sind die *Verträge mit Geschäftspartnern, die Geschäftsgeheimnisse tangieren,* daraufhin zu überprüfen, ob das in diesem Zusammenhang gegebenenfalls zugänglich gemachte oder weitergegebene Know-how angemessen vor Offenlegung, Missbrauch und Reverse Engineering geschützt ist. Dazu gehört die Überarbeitung und Aktualisierung von Vertraulichkeits- wie auch Rechtseinräumungsklauseln in Standardverträgen.

Wenn dieses Pflichtenprogramm sorgfältig ausgearbeitet und umgesetzt wird, ist es zukünftig möglich, Algorithmen wie auch Daten(bestände) für sich und unabhängig von ihrer Einbettung in Big Data Anwendungen – aber auch speziell für diese – und Computerprogrammen zu sichern. Geschäftsgeheimnis-RL und ihr folgend der GeschgG-RegE stellen den Unternehmen hierfür die notwendigen Möglichkeiten und Anspruchsgrundlagen sowie angemessene Mittel der Rechtsdurchsetzung zur Verfügung. Es wäre fahrlässig, diese nicht zu nutzen.

Dr. Katharina Scheja

Rechtsanwältin & Lehrbeauftragte an der Universität Göttingen, Of-Counsel der Kanzlei Deloitte Legal GmbH

Informationstechnologie, Intellectual Property & Outsourcing

kscheja@deloitte.de

Rechtsprechung

OLG Hamm: Eigenhändler beim software-unterstützten Online-Handel mit Finanzprodukten

KWG §§ 1 Abs. 1a Satz 2 Nr. 3, 32 Abs. 1 Satz 1; BGB §§ 134, 142, 280 Abs. 1, 812 Abs. 1, 823 Abs. 2

Beim automatisierten Internethandel mit Finanzprodukten mittels einer Software liegt ein Eigenhandel desjenigen vor, der über die grundlegenden Einstellungen und Vorgaben entscheidet. Nicht entscheidend ist, wer die Einstellungen und Vorgaben – auf der Grundlage dieser Entscheidung – tatsächlich dem Programm vorgibt und ob die Software auf einem Computer des Entscheidenden installiert ist. *(amtl.)*

OLG Hamm, Urt. v. 30.5.2018 – I – 12 U 95/16
(LG Paderborn, Urt. v. 12.5.2016 – 3 O 290/15)

Aus dem Sachverhalt:

A. Der Kläger macht gegen den Beklagten Schadensersatzansprüche im Hinblick auf Verluste geltend, die ihm beim sog. Forex-Handel entstanden sind.

Der Beklagte betreibt als Einzelkaufmann eine Wirtschaftsberatung. Im Juli 2013 kam es auf Empfehlung der Zeugin X zu einem Gespräch des Beklagten mit dem Kläger (...). Gegenstand des Gesprächs war der Wunsch des Klägers (...), größere Geldbeträge gewinnbringend anzulegen. Der Beklagte stellte dem Kläger (...) die Möglichkeit eines automatischen Handels mit Währungen im Devisenmarkt, des sog. Forex-Handels, mit der von ihm entwickelten Software Expert Advisor vor.

Mit Email vom 27.9.2013 teilte der Beklagte dem Kläger mit: „Vereinbarung EA 3.0 (automatisches Forex-Trading – Basis N 4) ... Wunschgemäß stellen wir Ihnen unseren o.g. EA für Ihr Forex-Trading zur Verfügung. Es wurde die reine Anmietung der Software vereinbart. (...)" (...)