Big Data und der europäische Rechtsrahmen:

Status quo und Reformbedarf im Lichte der Trade-Secrets-Richtlinie 2016/943/EU*

*Thomas Sagstetter***

---

* Dieser Beitrag basiert auf einem Vortrag, den der Verf. im Rahmen der vierten Tagung GRUR Junge Wissenschaft am 30. Juni 2018 an der Technischen Universität München (TUM) gehalten hat. Der Beitrag wird demnächst im entsprechenden Tagungsband veröffentlicht. Die Open-Access-Vorabveröffentlichung erfolgt mit freundlicher Genehmigung des NOMOS Verlages.

** Wiss. Mitarbeiter am Lehrstuhl für Bürgerliches Recht und Recht des Geistigen Eigentums mit Informationsrecht und IT-Recht (GRUR-Lehrstuhl) und Doktorand bei Prof. Dr. jur. Dr. h.c. Peter Kindler am Institut für Internationales Recht der Ludwig-Maximilians-Universität München. Mein besonderer Dank gilt *Prof. Dr. Matthias Leistner, LL.M. (Cambridge)* für die vielen fruchtbaren Diskussionen zur Thematik dieses Beitrags. Überdies danke ich den Mitgliedern der Forschungsgruppe „Datengetriebene Wirtschaft: Regulierungsbedarf infolge von Digitalisierung“ am Max-Planck-Institut für Innovation und Wettbewerb in München für den wertvollen Gedankenaustausch und unseren studentischen Mitarbeitern für ihre wertvolle Hilfe bei der Recherche und dem Korrekturlesen des Manuskripts.

A. Einleitung

Die Trade-Secrets-Richtlinie[1] wird das bislang divergierende nationale Recht des Geheimnisschutzes in weiten Teilen harmonisieren.[2] Allerdings zielte der Unionsgesetzgeber bei der Schaffung des neuen Rechtsaktes nicht darauf ab, den Besonderheiten und Belangen der informations- bzw. datengetriebenen Wirtschaft Rechnung zu tragen.[3] Stattdessen hauchte er der neuen Richtlinie den Geist des vergangenen Jahrhunderts ein, indem er breite Anleihen beim TRIPS-Abkommen aus den neunziger Jahren nahm.

Dieser Befund erstaunt, haben sich doch die Rolle und das Potential von Informationen bzw. Daten[4] in Wissenschaft, Wirtschaft und Gesellschaft in den letzten Jahren erheblich verändert.[5] Vor diesem Hintergrund steht die Anpassung des europäischen Rechtsrahmens an die Entwicklungen im Bereich der datengetriebenen Wirtschaft eigentlich im Fokus europäischer Rechtssetzungs-, Revisions- und Evaluationsbemühungen.[6] Die stiefmütterliche Behandlung des Geheimnisschutzes lässt sich nur damit erklären, dass dessen Bedeutung für die europäische Datenwirtschaft[7] bislang erheblich unterschätzt wurde.[8]

Dieser Beitrag wird offenlegen, dass das neue Geheimnisschutzregime in typischen Sachverhalten im Kontext der Datenwirtschaft weitreichende Schutzrechte an Daten, Algorithmen und neuronalen Netzen begründet und damit zugleich in einem besonderen

---

1 RL 2016/943/EU des Europäischen Parlaments und des Rates v. 8.6.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. 2016 L 157, 1 (Trade-Secrets-Richtlinie). Bemerkenswerterweise wurde in den USA nahezu zeitgleich mit dem Defend Trade Secrets Act of 2016 ein einheitliches Geheimnisschutzregime auf Bundesebene geschaffen, vgl. *Lejeune*, CR 2016, 330, 339 ff. mwN. Aus Platzgründen kann im Rahmen des Beitrags nicht auf die interessanten weiteren Parallelen eingegangen werden. Zur Revision des japanischen Unfair Competition Prevention Acts unten Fn. 157.

2 Zur bisherigen Rechtslage in den einzelnen Mitgliedstaaten vgl. *Niebel*, in: FS Fezer, 2016, S. 799, 807-808 mwN insb. zu den im Auftrag der Kommission durchgeführten Studien; zum differenzierenden Harmonisierungskonzept der Richtlinie s. unten bei Fn. 10.

3 Vgl. dazu *Drexl/Hilty/Desaunettes et al.*, GRUR Int. 2016, 914, 916-917.

4 Zu den schillernden (Rechts-)Begriffen „Daten" und „Informationen" vgl. statt vieler *Zech*, Information als Schutzgegenstand, 2012, S. 32; *Determann*, UC Hastings Research Paper No. 265, 2018, 1, 6-7 mwN; *Becker*, GRUR 2017, 346, 347 mwN. Zur problematischen Abgrenzung zwischen Zeichen- bzw. Bedeutungsebene vgl. *Drexl*, NZKart 2017, 339, 343 mwN.

5 Zur Bedeutung heute meist in elektronischer Form gespeicherter geheimer Informationen und der damit einhergehenden erhöhten Verletzlichkeit von Geschäftsgeheimnissen s. statt vieler *Hohendorf*, in: Hennemann/Sattler, Immaterialgüter und Digitalisierung, 2017, S. 105, 105-106 mwN; *Niebel/Lorenzo/Clark*, JIPLP 2018, 445, 446-447, 454 mwN. Zu den spezifischen Gefahren für Geschäftsgeheimnisse in Industrie 4.0-Umgebungen s. *Müllmann*, WRP 2018, 1177, 1179 ff. mwN.

6 Vgl. bereits COM(2014) 442 endg.; COM(2015) 192 endg., 4, 16; COM(2017) 9 endg. mit begleitendem SWD(2017) 2 endg.; COM(2017) 228 endg.; COM(2017) 495 endg.; jüngst: COM(2018) 232 endg. mit begleitendem SWD(2018) 125 endg. sowie zur Evaluation der Datenbankrichtlinie im Kontext der Datenwirtschaft zurückhaltend SWD(2018) 146 endg., insb. 35-40 je mwN. Zu den Friktionen zwischen der Initiative „Aufbau einer europäischen Datenwirtschaft" und dem Vorschlag für eine Richtlinie über das Urheberrecht im digitalen Binnenmarkt (COM(2016) 593 endg.): *Raue*, IIC 2018, 379 ff. mwN.

7 Zu dem Begriff der Datenwirtschaft und den schillernden Begriffen *Big Data*, *Artificial Intelligence*, *Smart Factory*, *Industrie 4.0*, etc. s. *Sagstetter*, in: Husemann/Korves/Rosenkranz et al., Jahrbuch Junger Zivilrechtswissenschaftler, 2018 (im Erscheinen).

8 Vgl. etwa COM(2017) 9 endg., 11 ff.: Die Kommission stellt nur fest, dass die von Maschinen erzeugten Rohdaten für sich genommen i.d.R. keinen Datenbank- oder Geheimnisschutz genießen, s. zum Schutz von Einzeldaten unten B. I. 4. Allgemein zur Rolle des Geheimnis- und Datenbankschutzes als „ungeliebte Stiefkinder" des Geistigen Eigentums *Ann*, GRUR 2007, 39; *Wiebe*, CR 2014, 1.

Spannungsverhältnis zu sonstigen Schutzinstrumenten und den Zielen des freien Datenflusses (*free flow of data*) bzw. des Zugangs zu Daten steht. Folglich wäre eine dezidierte Abstimmung der Richtlinie mit den Besonderheiten des digitalen Zeitalters und dem bestehenden *acquis communautaire* eminent wichtig und wünschenswert gewesen. Zwar ist mit einer Revision der Richtlinie auf absehbare Zeit nicht zu rechnen.[9] Jedoch sollten die Mitgliedstaaten ihre vorhandenen Umsetzungsspielräume[10] nutzen, um wenigstens auf nationaler Ebene ein Geheimnisschutzregime zu etablieren, das dem digitalen Zeitalter möglichst adäquat Rechnung tragen kann. Es bleibt abzuwarten, ob dies unionsweit gelingen wird. Der aktuelle Stand des Umsetzungsprozesses in Deutschland stimmt jedenfalls nicht optimistisch. So zielen der Referentenentwurf und der jüngst veröffentlichte Regierungsentwurf ebenso wenig wie die Richtlinie darauf ab, den Besonderheiten und Bedürfnissen der Datenwirtschaft gerecht zu werden.[11]

Spätestens im Rahmen der richtlinienkonformen Auslegung des jeweiligen nationalen Geheimnisschutzregimes werden diese Besonderheiten und Bedürfnisse jedoch Berücksichtigung finden müssen. Denn obgleich der Gesetzgeber mit der Richtlinie nicht auf eine spezifische Regulierung der datengetriebenen Wirtschaft abzielte, wollte er doch einen flexiblen Rechtsrahmen schaffen, der an dynamische, technische und wirtschaftliche Entwicklungen anpassbar bleibt.[12]

Die kritische Analyse des neuen Rechtsaktes fügt sich darüber hinaus in einen allgemeineren Rahmen: Lässt sich der bestehende *acquis communautaire* an die Besonderheiten und

---

[9] Vgl. Art. 18 Abs. 3. Der Referentenentwurf des BMJV – Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (im Folgenden: RefE) hielt eine eigenständige nationale Evaluierung nicht für erforderlich (S. 18). Der Regierungsentwurf (im Folgenden: RegE) sieht nun ein eigenständiges nationales Evaluierungsverfahren vor, das diejenigen Regelungen betreffen soll, die über die 1:1-Umsetzung der Richtlinie hinausgehen (S. 20). RefE und RegE sind abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/GeschGehG.html [alle Internetquellen wurden zuletzt am 1.10.2018 abgerufen]. Zum aktuellen Stand vgl. https://rsw.beck.de/aktuell/gesetzgebung/gesetzgebungsvorhaben-entwicklungsgeschichte/schutz-von-geschaeftsgeheimnissen mwN sowie *Dumont*, BB 2018, 2441 ff.; *Brammsen*, BB 2018, 2446 ff. Ein bündiger Vergleich zwischen RefE und RegE findet sich bei *Müllmann*, WRP 2018, 1177, 1181.

[10] Die Trade-Secrets-Richtlinie folgt einem differenzierenden Harmonisierungsansatz, vgl. *Alexander*, WRP 2017, 1034, 1036 mwN. Im Grundsatz ist sie mindestharmonisierend, Art. 1 Abs. 1 UAbs. 2. Einige Artikel haben allerdings vollharmonisierende Wirkung. Dies gilt zum einen für die in Art. 1 Abs. 1 UAbs. 2 explizit genannten und zum anderen für diejenigen Artikel, deren vollharmonisierende Wirkung implizit vorausgesetzt wird, vgl. *Ackermann/Rindell*, GRUR Int. 2017, 486, 487; zur vollharmonisierenden Wirkung des Art. 2 Nr. 1 s. unten Fn. 14. Zur Kritik am Harmonisierungsansatz der Richtlinie unten C.

[11] Aus Platzgründen kann nicht vertieft auf den RefE und den RegE eingegangen werden. In den Fußnoten wird an den entscheidenden Stellen auf den RefE/RegE Bezug genommen. Zu dem Begriff der „Unternehmensdaten“ im RefE/RegE vgl. unten Fn. 144. Der RegE basiert insgesamt auf einer Fehleinschätzung. So heißt es auf S. 19 ohne nähere Begründung, dass bei einer nicht unbeträchtlichen Zahl von Betrieben keine Geschäftsgeheimnisse vorhanden sind bzw. nur etwa 20 Prozent der Kleinstunternehmen über Informationen verfügen, bei denen ein Geheimnisschutz in Betracht kommt. Dies kann insbesondere vor dem Hintergrund der weiten Definition des Schutzgegenstandes nicht überzeugen, vgl. unten B. I. Kritisch zum prognostizierten Mehraufwand für Unternehmen bzw. Justiz *Ziegelmayer*, CR 2018, 693, 694; *Brammsen*, BB 2018, 2446, 2447.

[12] Vgl. *Drexl/Hilty/Desaunettes et al.*, GRUR Int. 2016, 914, 917.

Bedürfnisse der europäischen Datenwirtschaft anpassen, entfällt bereits im Ausgangspunkt jede Rechtfertigung für die Einführung neuer Schutzrechte.[13]

B. Die Relevanz der Trade-Secrets-Richtlinie für die europäische Datenwirtschaft de lege lata und de lege ferenda

I. Schutzgegenstand

1. Weite Definition des Geschäftsgeheimnisses gem. Art. 2 Nr. 1

Dreh- und Angelpunkt der Trade-Secrets-Richtlinie ist die Legaldefinition des Geschäftsgeheimnisses in Art. 2 Nr. 1, die sich eng an Art. 39 Abs. 2 TRIPS anlehnt.[14] Danach sind Informationen als Geschäftsgeheimnisse zu qualifizieren, sofern sie drei kumulative Voraussetzungen erfüllen:

- sie sind in dem Sinne geheim, dass sie [ent]weder in ihrer Gesamtheit [oder] in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, [nicht] allgemein bekannt oder ohne weiteres zugänglich sind,[15]
- sie sind von kommerziellem Wert, weil sie geheim sind,
- sie sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt.

---

[13] Für die Einführung neuer Ausschließlichkeitsrechte an Daten vgl. statt vieler jüngst *Fezer*, Repräsentatives Dateneigentum, 2018, S. 45 ff. mwN; *Amstutz*, AcP 2018, 438, 479 ff.; *Tjong Tjin Tai*, EuCML 2018, 136 ff.; *Mayer*/*Ritter*, Duke L. & Tech. Rev. 2018, 220, 223 ff. Vgl. für einen Überblick über den Meinungsstand und eine kritische Würdigung dieser Ansichten *Sagstetter*, in: (Fn. 7) mwN (im Erscheinen).

[14] Zu Art. 39 Abs. 2 TRIPS vgl. Erwägungsgründe 5 und 6. Art. 39 TRIPS ist seinerseits vom US-amerikanischen Uniform Trade Secrets Act inspiriert, vgl. zur Entstehungsgeschichte ausführlich *Sandeen*, in: Strandburg/Dreyfuss, The law and theory of trade secrecy, 2011, S. 537, 539 ff. mwN; Busche/Stoll/Wiebe/*Peter/Wiebe*, 2. Aufl., Art. 39 TRIPS Rn. 1-9 mwN. Kritisch zur Anlehnung an Art. 39 Abs. 2 TRIPS u.a. *Harte-Bavendamm*, in: FS Köhler, 2014, S. 235, 240. Das Telos der Richtlinie – Innovationsförderung durch grenzüberschreitenden Geheimnisschutz – spricht für eine unionsweite einheitliche Definition des zentralen Begriffs „Geschäftsgeheimnis". Art. 2 Nr. 1 sollte daher als vollharmonisierend verstanden werden, vgl. auch Erwägungsgrund 14, der betont, es sei wichtig eine „[…] homogene Definition des Begriffs „Geschäftsgeheimnis" festzulegen […]". In diese Richtung statt vieler auch: *Harte-Bavendamm*, in: FS Büscher, 2018, S. 311, 312-314 mwN; *Ackermann/Rindell*, GRUR Int. 2017, 486, 487; a.A.: Österreichischer OGH, Urt. v. 25.10.2016 – 4 Ob 165/16t, BeckRS 2016 117117 (s. dazu unten bei Fn. 73); *Lejeune*, CR 2016, 330, 333 i.V.m. 331.

[15] Die deutsche Fassung der Richtlinie wurde fehlerhaft übersetzt, weshalb die hier vorgenommenen Korrekturen in eckigen Klammern erforderlich sind, vgl. dazu die Stellungnahme des Max-Planck-Instituts für Innovation und Wettbewerb zum Referentenentwurf eines Gesetzes zur Umsetzung der Richtlinie, 30.5.2018, S. 3-4 (im Folgenden: MPI-Stellungnahme 2018). Die fehlerhafte Übersetzung wurde sowohl in den RefE als auch in den RegE übernommen. Zu weiteren Übersetzungsungenauigkeiten in der deutschen Fassung der Richtlinie bzw. Widersprüchen zu anderen Sprachfassungen *Wiese*, Die EU-Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen, 2018, S. 42 ff.

Diese dreiteilige Definition des Schutzgegenstandes ist weit gefasst. Überdies legt Erwägungsgrund 14 eine extensive Auslegung nahe. Er betont einleitend, dass es wichtig sei, eine homogene Definition festzulegen, ohne den vor widerrechtlicher Aneignung zu schützenden Bereich einzuengen.

Insbesondere das Kriterium des kommerziellen Werts ist im Lichte der Erwägungsgründe denkbar weit zu verstehen. So muss die fragliche Information keinen realen Handelswert verkörpern; ein potentieller Wert genügt. Die Richtlinie legt nicht abschließend fest, wie dieser potentielle Wert zu bemessen ist. Stattdessen weist Erwägungsgrund 14 S. 4 nur beispielhaft auf einen prospektiv-schadenszentrierten Bemessungsansatz hin: Eine Information verkörpert einen Handelswert, wenn ihre widerrechtliche Aneignung die Interessen des Inhabers des Geschäftsgeheimnisses aller Voraussicht nach dadurch schädigt, dass das wissenschaftliche oder technische Potential, die geschäftlichen oder finanziellen Interessen, die strategische Position oder die Wettbewerbsfähigkeit dieser Person untergraben werden. Daneben sind mindestens zwei weitere Ansätze zur Bemessung des kommerziellen Werts denkbar. Zum einen könnte man auf die Investitionen abstellen, die zur Beschaffung bzw. Generierung der Informationen erforderlich waren (investitionszentrierter Ansatz);[16] zum anderen auf eine fiktive Marktnachfrage nach den jeweiligen Informationen (marktzentrierter Ansatz).[17] Die Information muss jedenfalls gerade deshalb von kommerziellem Wert sein, weil sie geheim ist. Dabei genügt es allerdings, wenn der kommerzielle Wert zumindest auch aus dem geheimen Charakter resultiert.[18] Eine derart weit verstandene Verbindung zwischen kommerziellem Wert und geheimem Charakter dürfte sich regelmäßig herstellen lassen.[19] Es fehlt somit an substantiell begrenzenden Kriterien in qualitativer oder quantitativer Hinsicht – etwa im Sinne einer Wesentlichkeitsschwelle. Das Merkmal des kommerziellen Wertes ist daher letztlich als *de-minimis*-Schwelle zu verstehen.[20] Dies bestätigt auch Erwägungsgrund 14 S. 5, der explizit nur belanglose Informationen von der Definition des Geschäftsgeheimnisses ausklammert.

2. Anknüpfungspunkte in typischen Big Data- und Industrie 4.0-Sachverhalten

Im Rahmen von Big Data- und Industrie 4.0-Sachverhalten werden eine Vielzahl von Informationen gesammelt, genutzt und geschaffen, die möglicherweise als Geschäftsgeheimnisse i.S.d. Richtlinie zu qualifizieren sind.[21]

---

[16] Vgl. zum Kriterium der Investition im Rahmen des *sui generis*-Rechts *Leistner*, in: Lohsse/Schulze/Staudenmayer, Trading data in the digital economy: legal concepts and tools, 2017, S. 27, 27-30 mwN.

[17] Vgl. *Sousa e Silva*, JIPLP 2014, 923, 930.

[18] Busche/Stoll/Wiebe/*Peter/Wiebe*, 2. Aufl., Art. 39 TRIPS Rn. 22; *Alexander*, WRP 2017, 1034, 1039.

[19] S. noch weitergehend: MPI-Stellungnahme 2018, S. 3: „automatisch". Zurückhaltender *Drexl*, JIPITEC 2017, 257, 269.

[20] Zugunsten eines weiten Verständnisses des Kriteriums statt vieler *Aplin*, in: (Fn.16), S. 59, 65-66; zum vergleichbaren – wenn auch noch weiter verstandenen – Kriterium „economic value of information" im Trade-Secrets-Recht der USA (Uniform Trade Secrets Act of 1979 [geändert 1985] sowie Defend Trade Secrets Act of 2016 [dazu bereits oben Fn. 1]) vgl. *Wennakoski*, EIPR 2016, 154, 156-157 mwN.

[21] Für eine ausführliche Untersuchung potentiell relevanter Rechtsobjekte im Rahmen typischer Big Data-Sachverhalte s. *Sagstetter*, in: (Fn. 7) mwN (im Erscheinen).

a) Einzeldatum

Die Kriterien des „kommerziellen Werts“ und des „geheimen Charakters“ erschweren es allerdings bereits im Ausgangspunkt, einzelne Daten als Geschäftsgeheimnis zu qualifizieren.

Zwar ist das Erfordernis des kommerziellen Werts – wie gezeigt – denkbar weit zu verstehen. Ein nicht kontextualisiertes Einzeldatum – beispielsweise der isolierte Messwert ‚27‘ ohne Metadaten[22] – hat jedoch bei marktzentrierter Betrachtungsweise für sich genommen keinen potentiell kommerziellen Wert.[23] Marktwert erhalten isolierte Einzeldaten vielmehr erst durch Aggregation und/oder Kombination mit Kontextinformationen. Auch bei prospektiv-schadenszentrierter Betrachtungsweise ist nicht ersichtlich, wie die widerrechtliche Aneignung eines isolierten Einzeldatums die Interessen des Inhabers des Geschäftsgeheimnisses schädigen könnte. Nur wenn man einen investitionszentrierten Maßstab anlegt und auf die spürbaren Kosten abstellt, die zur Beschaffung oder Generierung des Einzeldatums erforderlich waren, könnte man einen potentiell wirtschaftlichen Wert bejahen.[24] Jedenfalls ist ein kontextloses Einzeldatum als „belanglose Information“ zu qualifizieren und daher nach Erwägungsgrund 14 S. 5 explizit von der Definition des Geschäftsgeheimnisses ausgenommen. Somit wird man ein Einzeldatum selbst dann nicht als Geschäftsgeheimnis i.S.d. Richtlinie qualifizieren können, wenn dessen Beschaffung oder Generierung mit spürbaren Investitionen verbunden ist.

Überdies ist fraglich, ob ein kontextloses Einzeldatum einen geheimen Charakter aufweisen kann. Dagegen spricht bereits der Wortlaut des Art. 2 Nr. 1 lit. a:[25] Die fragliche Information muss „in ihrer Gesamtheit [oder] in der genauen Anordnung und Zusammensetzung ihrer Bestandteile“ geheim sein. Bei einem isolierten Einzeldatum kann man aber schwerlich von einer „Gesamtheit“ oder von „Bestandteilen“ sprechen. Zudem sind gesammelte oder abgegriffene Einzeldaten häufig öffentlich zugänglich und können insoweit keinen geheimen Charakter i.S.d. Art. 2 Nr. 1 lit. a aufweisen.[26]

b) Datensets

In Big Data- und Industrie 4.0-Sachverhalten bietet sich allerdings kraft Natur der Sache ein weiterer Anknüpfungspunkt an: Das einzelne Datum wird in solchen Sachverhalten notwendigerweise mit anderen Daten kombiniert und kontextualisiert in ein Datenset überführt. Denn erst aus einem Datenset lassen sich mit Hilfe von (Big Data-)Algorithmen potentiell Erkenntnisse ableiten, die in Ansehung einzelner Daten nicht zu vermuten wären.[27] Auf Basis dieser Erkenntnisse können neue Produkte oder Dienstleistungen entwickelt oder bestehende verbessert werden. Somit kann ein Datenset indirekt als Grundlage künftiger Wertschöpfung dienen. Da es im Übrigen an begrenzenden Kriterien in qualitativer oder quantitativer Hinsicht

---

22 Zur Abgrenzung von Primär- und Metadaten *Krüger*/*Möllers*, MMR 2016, 728 mwN.

23 In diese Richtung auch *Aplin*, in: (Fn. 16), S. 59, 66.

24 Für einen potentiell wirtschaftlichen Wert eines Einzeldatums bei spürbaren Kosten im Rahmen der Datengenerierung *Drexl/Hilty/Desaunettes et al.*, GRUR Int. 2016, 914, 916.

25 Ebenso *Aplin*, in: (Fn. 16), S. 59, 66.

26 *Drexl/Hilty/Desaunettes et al.*, GRUR Int. 2016, 914, 916 mit instruktivem Bsp.

27 S. dazu statt vieler *Fries*, NJW 2016, 2860, 2862 Fn. 28 sowie *Mayer-Schönberger/Cukier*, Big Data, 2017, S. 13 ff.

fehlt,[28] ist nach allen Bemessungsmethoden (markt-, investitions- und prospektiv-schadenszentriert) ein potentieller kommerzieller Wert eines jeden Datensets zu bejahen. Ob dem Datenset unstrukturierte Rohdaten (bloßer Datenhaufen) oder strukturierte Daten zugrunde liegen, ist unerheblich, weil sich selbst aus unstrukturierten Rohdaten ein – wenn auch geringer – potentiell kommerzieller Wert gewinnen lässt.[29] Unschädlich ist es auch, wenn das Datenset teilweise oder insgesamt aus öffentlich zugänglichen Informationen besteht. Denn aus der konkreten Kombination der (Meta-)Daten im jeweiligen Datenset lassen sich neue Erkenntnisse ableiten und damit potentieller kommerzieller Wert schöpfen. Vor diesem Hintergrund kommt es nicht darauf an, ob das Datenset neben nicht-personenbezogenen Daten auch solche mit Personenbezug enthält.[30]

Datensets könnten allenfalls als „belanglose Informationen" vom Schutzbereich ausgeschlossen sein. Allerdings lassen sich aus einem Datenset mittels (Big Data-)Algorithmen belangvolle Erkenntnisse ableiten – selbst wenn es für sich genommen nur belanglose Informationen enthält. Voraussetzung ist nur, dass in dem Datenset genug belanglose Informationen zusammengefügt sind[31] oder das Datenset mit anderen Daten kombiniert bzw. durch Metadaten kontextualisiert wird. Daher kommt – bei der aus teleologischer Perspektive gebotenen Gesamtbetrachtung – der Ausschluss eines Datensets als „belanglose Information" nur in absoluten Ausnahmefällen in Betracht.[32]

Als Zwischenergebnis bleibt somit festzuhalten: Datensets sind regelmäßig von potentiell kommerziellem Wert.[33] Gleiches gilt für neue Informationen, die aus den Datensets abgeleitet wurden.

Die Frage nach dem geheimen Charakter eines Datensets lässt sich nur in negativer Hinsicht pauschal beantworten. Am geheimen Charakter fehlt es jedenfalls dann, wenn das Datenset in seiner Gesamtheit frei verfügbar ist – etwa durch eine Veröffentlichung im Rahmen der Open-Data-Bewegung.[34] Handelt es sich dagegen um nicht frei verfügbare Datensets, ist die maßgebliche Frage, ob sie in ihrer Gesamtheit oder genauen Anordnung und Zusammensetzung allgemein bekannt oder ohne weiteres zugänglich sind. Dabei ist auf den Personenkreis abzustellen, der üblicherweise mit Informationen der jeweiligen Art umgeht. Vor diesem

---

[28] Zur regelmäßig vorliegenden Verbindung zwischen kommerziellem Wert und geheimem Charakter vgl. oben B. I. 1.

[29] *Zech*, JIPLP 2016, 460, 465; *Alexander*, WRP 2017, 1034, 1038; vgl. auch *Grützmacher*, CR 2016, 485, 488.

[30] Selbst öffentlich zugängliche personenbezogene Daten haben kraft ihrer Kombinationsmöglichkeit mit anderen Daten potentiell kommerziellen Wert. Zum möglichen Schutz personenbezogener Daten durch die Richtlinie bereits Annex 21 des SWD(2013) 471 endg., 254; zum potentiellen Wert personenbezogener Daten am Beispiel von Online-Plattformen *Graef*, World Competition 2015, 473, 482; vgl. auch *Alexander*, WRP 2017, 1034, 1038 am Beispiel von „intelligenten" Mess-Systemen (*Smart Meter*). Zur schwierigen Unterscheidung von Personen- und Sachdaten im Kontext der Datenwirtschaft *Sagstetter*, in: (Fn. 7) mwN (im Erscheinen). Zur Interaktion von Geheimnis- und Datenschutz vgl. unten Fn. 152.

[31] Vgl. *Zech*, JIPLP 2016, 460, 465.

[32] In diese Richtung bereits allgemein BVerfG, NJW 1984, 419, 422 – Volkszählungsurteil: „[…] unter den Bedingungen der automatischen Datenverarbeitung [gibt es] kein „belangloses" Datum mehr.".

[33] *Drexl/Hilty/Desaunettes et al.*, GRUR Int. 2016, 914, 917; *Aplin*, in: (Fn. 16), S. 59, 66 (im Hinblick auf nicht-personenbezogene Daten); zur bisherigen autonomen Rechtslage in Deutschland *Sattler*, in: Sassenberg/Faber, Rechtshandbuch Industrie 4.0, 2017, S. 27, 37-38 mwN.

[34] Ebenso speziell zur Open-Data-Bewegung *Aplin*, in: (Fn. 16), S. 59, 66 mwN.

Hintergrund herrscht Einigkeit, dass die Informationen nicht „absolut", sondern nur „relativ" geheim sein müssen.[35]

Prima facie ist die Bestimmung dieses geheimen Charakters in Big Data-Sachverhalten besonders schwierig, denn die in diesem Rahmen genutzten bzw. erzeugten Datensets zeichnen sich typischerweise durch eine besondere Vielfalt (Variety) aus.[36] Für Big Data-Datensets ist allerdings ebenso charakteristisch, dass sie aus aggregierten, kombinierten und mittels Metadaten kontextualisierten Einzeldaten bestehen. Kraft dieser kontextuellen Zusammenstellung ist ein solches Datenset regelmäßig weder in seiner Gesamtheit noch in seiner genauen Anordnung oder Zusammensetzung allgemein bekannt bzw. ohne weiteres zugänglich.[37] Gleiches gilt für die aus den Datensets abgeleiteten neuen Informationen.

So können beispielsweise Informationen über Nutzer, Kunden oder Geschäftspartner für sich betrachtet allgemein bekannt bzw. ohne weiteres zugänglich sein.[38] Werden diese Daten aber aggregiert, miteinander kombiniert und kontextualisiert, ist das entstandene Datenset in seiner Gesamtheit bzw. seiner konkreten Zusammenstellung in der Regel nicht öffentlich zugänglich. In dieser – für Big Data-Sachverhalte typischen Konstellation – weist das betreffende Datenset somit einen geheimen Charakter i.S.d. Richtlinie auf.[39] Gleiches gilt für neue Erkenntnisse, die aus dem Datenset abgeleitet werden, wie beispielsweise das (prognostizierte) Kaufverhalten einer bestimmten Kundengruppe[40]. Ebenso weisen Datensammlungen, wie sie etwa im Kontext von Text- und Data-Mining[41] oder im Zusammenhang mit dem Training Künstlicher Intelligenz (maschinelles Lernen) aggregiert, normalisiert und strukturiert werden (sog. Korpora[42]), regelmäßig einen geheimen Charakter auf. Dies gilt entsprechend für neuronale Netze und separat gespeicherte Gewichtungsmatrizen, die im Rahmen maschinellen Lernens entstehen.[43]

---

35 Vgl. *Sousa e Silva*, JIPLP 2014, 923, 928-929 mwN.

36 *Aplin*, in: (Fn. 16), S. 59, 67; vgl. zu den für Big Data-Sachverhalte charakteristischen „3 V's": Volume (große Datenmengen im Tera- bis Zettabytebereich [Terabyte = 10^{12} Byte, Zettabyte = 10^{21} Byte]), Variety (Vielfalt von strukturierten, semi-strukturierten und unstrukturierten Daten) und Velocity (hohe Verarbeitungsgeschwindigkeit) *Fasel/Meier*, in: Fasel/Meier, Big Data, 2016, S. 3, 5-6 mwN (dort auch zu den von einigen zur Definition hinzugefügten beiden weiteren V's: Value und Veracity).

37 Ebenso *Drexl/Hilty/Desaunettes et al.*, GRUR Int. 2016, 914, 916-917.

38 Vgl. *Graef*, World Competition 2015, 473, 482. Abonnentenlisten in den sozialen Netzwerken ähneln zwar prima facie Kundenlisten (zu diesem allgemein anerkannten Beispiel eines Geschäftsgeheimnisses sogleich Fn. 39); wegen ihrer Verfügbarkeit im Internet haben sie aber i.d.R. keinen geheimen Charakter vgl. *Surblyte*, GRUR Int. 2016, 1121, 1123 ff., 1128 mwN. Generell zum geheimen Charakter von Informationen, die im Internet veröffentlicht wurden *Cundiff*, IDEA 2009, 359, 395-409 mwN (aus Sicht des Trade-Secrets-Rechts der USA).

39 Vgl. dazu *Drexl/Hilty/Desaunettes et al.*, GRUR Int. 2016, 914, 916-917; zu dem ähnlich gelagerten allgemein anerkannten Beispiel einer Kundenliste vgl. bereits Annex 21 des SWD(2013) 471 endg., 254.

40 Vgl. dazu die konkreten Beispiele bei *Mayer-Schönberger/Cukier*, Big Data, 2017, S. 71 ff., 76 ff. mwN.

41 Zum Begriff des Text- und Data-Minings und dessen Bedeutung für Big Data-Analysen sowie einer Zusammenfassung der Rechtslage *Raue*, GRUR 2017, 11, 13 mwN.

42 Vgl. zu Begriff und Bedeutung der Korpora *Truyens*/*Eecke*, CLSR 2014, 153, 154 ff. mwN.

43 Ebenso im Hinblick auf neuronale Netze *Surblyte*, WUW 2017, 120, 125. Vgl. sehr gut verständlich zu den technischen Grundlagen der Künstlichen Intelligenz *Stiemerling*, CR 2015, 762 ff.; speziell zu den technischen Grundlagen des maschinellen Lernens *Ehinger*/*Stiemerling*, CR 2018, 761, 762 ff., 769 mit den Hinweis, dass separat gespeicherte Trainingsergebnisse [= strukturierte Informationen über die Gewichtung der Synapsen (Gewichtungsmatrizen)] grundsätzlich Geheimnisschutz genießen können. Der Einfachheit halber wird im Folgenden nur von neuronalen Netzen gesprochen.

Da Art. 2 Nr. 1 lit. a keine begrenzenden Kriterien in qualitativer oder quantitativer Hinsicht kennt, ist es unerheblich, wie hoch der Strukturierungs- bzw. Kontextualisierungsgrad der entsprechenden Datensets ist bzw. wie viele Einzeldaten das Datenset enthält. Daher sind auch bloße Datenhaufen in der Regel als geheim zu qualifizieren, weil die aggregierten Rohdaten in ihrer genauen Zusammensetzung regelmäßig weder allgemein bekannt noch ohne weiteres zugänglich sind. Somit werden auch Rohdatensets – wie sie beispielsweise im Kontext der Vernetzung bei Industrie 4.0, dem Internet of Things (IoT) oder bei Connected Cars gesammelt werden – regelmäßig einen geheimen Charakter aufweisen.[44]

Datensets sind vor diesem Hintergrund für sich betrachtet regelmäßig geheim i.S.d. Art. 2 Nr. 1 lit. a. Zwar dürfte man intuitiv davon ausgehen, dass sie ihren geheimen Charakter verlieren, wenn sie – wie heutzutage häufig – auf fremden Servern (Outsourcing oder Cloud) gespeichert werden.[45] Wie gezeigt genügt es jedoch, wenn die betreffenden Datensets relativ geheim bleiben. Dies ist im Grundsatz selbst dann der Fall, wenn ein Outsourcing-Unternehmen oder ein Cloud-Anbieter direkten Zugriff auf die gespeicherten Datensets erhält.[46] Gleiches gilt für den (partiellen) Austausch im Rahmen kooperativer Netzwerke.[47] Unklar bleibt allerdings, wie vielen Personen Zugriff auf ein Datenset eingeräumt werden darf, ohne dass dessen geheimer Charakter verloren geht.[48] Aus dem Sinn und Zweck der Richtlinie – Innovationsförderung durch Geheimnisschutz[49] – lässt sich allerdings ableiten, dass der relativ geheime Charakter fortbesteht, wenn und soweit die Ausweitung des Kreises (potentieller) Mitwisser durch den konkreten Zweck der jeweiligen Unternehmung gerechtfertigt ist.[50] Andernfalls besteht die Gefahr, dass Unternehmen um der Geheimhaltung willen Kooperation bzw. Outsourcing auf ein Minimum reduzieren. Dies wäre gerade im Bereich Big Data misslich, denn hier verspricht eine vernetzte und verteilte Kooperations- und Wertschöpfungskette besonders innovative Erkenntnisse.

---

[44] Ähnlich speziell zu Datensets, die im Rahmen des Internet of Things (IoT) erzeugt werden *Radoń*, Trade Secrets Protection for 'Big Data', 2015, S. 35-36.

[45] Vgl. nur *Grützmacher*, CR 2016, 485, 489; zur Bedeutung cloudbasierter Lösungen für IoT *Surblyte*, WUW 2017, 120, 125. Zahlreiche Big Data-Anwendungen arbeiten darüber hinaus auf Basis verteilter Netzwerkstrukturen, d.h. die Daten werden räumlich verstreut und mehrfach auf verschiedenen Servern gespeichert, vgl. bspw. das Hadoop Distributed Filesystem (HDFS), ausführlicher dazu *Wiebe*, GRUR 2017, 338, 340.

[46] Erstens entfällt der relativ geheime Charakter hierdurch grundsätzlich nicht, zweitens werden Outsourcing-Unternehmen und insb. Cloud-Anbieter häufig nicht zu dem Personenkreis i.S.d. Art. 2 Nr. 1 lit. a gehören. Werden die Daten verschlüsselt in der Cloud gespeichert, bleiben sie sogar absolut geheim. Vgl. zur cloudbasierten Speicherung *Surblyte*, WUW 2017, 120, 125; *Sandeen*, Virginia Journal of Law and Technology 19 (2014), 1, 41 ff. (aus Sicht des Trade-Secrets-Rechts der USA).

[47] Zur Bedeutung von Geschäftsgeheimnissen für den Wissensaustausch i.R.v. kooperativer Forschung bzw. i.R.v. Open Innovation vgl. Erwägungsgrund 3.

[48] Vgl. hierzu sowie zum Fehlen international einheitlicher Standards *Surblyte*, in: Ullrich/Hilty/Lamping et al., TRIPS plus 20, 2016, S. 725, 737-738 mwN.

[49] Vgl. Erwägungsgründe 1-4, 8; allgemein zur umstrittenen theoretischen Rechtfertigung des Geheimnisschutzes vgl. *Ohly*, GRUR 2014, 1, 2-3 mwN; *Lemley*, Stan. L. Rev. 2008, 311, 312-314, 319 ff.; zur persönlichkeitsrechtlichen Theorie („personhood approach") *Graves*, J. Intell. Prop. L. 2007, 39, 70-73 mwN. Differenzierend zur Innovationsförderung durch Geheimnisschutz *Surblyte*, in: (Fn. 48), S. 725, 734-735 mwN.

[50] Unter dem Vorbehalt, dass sich der Kreis der Geschäftspartner nicht mit dem Personenkreis deckt, der üblicherweise mit Informationen der jeweiligen Art umgeht. Als Kompromiss zwischen Geheimhaltung und Kooperation bieten sich insb. Algorithm-to-the-data-Methoden an, vgl. COM(2018), 232 endg., 17 (übertragbar auf das B2B-Verhältnis).

c) Big Data-Algorithmen und Software-Implementierungen

Algorithmen[51], die im Rahmen von Big Data-Analysen eingesetzt werden, sind in der Regel ebenfalls geheim und zudem von kommerziellem Wert, denn nur durch ihren Einsatz lassen sich Datensets so verarbeiten und veredeln, dass aus ihnen neue Erkenntnisse abgeleitet werden können.[52] Deshalb sind Algorithmen dem Wortlaut des Art. 2 Nr. 1 nach grundsätzlich als Geschäftsgeheimnisse zu qualifizieren.[53] Dieser weitgehende Schutz von Algorithmen erstaunt,[54] widerspricht er doch der gesetzgeberischen Grundentscheidung, abstrakte Methoden, Ideen und Lehren gemeinfrei zu halten.[55] Allerdings sprechen für den Geheimnisschutz von Algorithmen gute Gründe: Hierdurch wird ein Anreiz für die – geheimniswahrende, da begrenzte – Offenlegung und gemeinsame Nutzung von Algorithmen gesetzt. Denn die Inhaber von Algorithmen können von strenger faktischer Geheimhaltung absehen, wenn und soweit sie sich auf den rechtlichen Geheimnisschutz verlassen können. Wird ein Algorithmus als Geschäftsgeheimnis qualifiziert, droht zudem stets ein Geheimnisverlust durch Reverse Engineering.[56] Dies setzt einen Anreiz, Algorithmen unter angemessenen Bedingungen offenzulegen bzw. sich auf eine Data-to-the-algorithm-Methode einzulassen.[57] Somit steht der Geheimnisschutz von Algorithmen in vollem Einklang mit dem Sinn und Zweck der Richtlinie.

Computerprogramme, die entsprechende Algorithmen implementieren, genießen ebenfalls im Grundsatz Geheimnisschutz.[58] Angesichts der weiten Definition des Schutzgegenstandes ist es nicht entscheidend, ob und inwieweit die Software bzw. die zugrundeliegenden Algorithmen durch den Menschen oder im Rahmen des maschinellen Lernens (fort-)entwickelt wurden. Wenn und soweit sie allerdings frei zugänglich werden,[59] entfällt ihr geheimer Charakter und damit der Geheimnisschutz.

---

[51] Zur allgemeinen Definition des Begriffs Algorithmus vgl. *Drexl/Hilty/Desaunettes et al.*, GRUR Int. 2016, 914, 916.

[52] Zurückhaltender *Surblyte*, WUW 2017, 120, 126; *Mattioli*, Minn. L. Rev. 2014, 535, 552-553 (aus Sicht des Trade-Secrets-Rechts der USA).

[53] Zum Schutz einer Score-Formel (= abstrakte Methode der Scorewertberechnung) als Geschäftsgeheimnis nach dem bisherigen autonomen deutschen Recht s. BGH NJW 2014, 1235, 1237 (insb. Rn. 17, 27-28) – Scoreformel (ohne nähere Begründung).

[54] Zur weiten Schutzwirkung des Geheimnisschutzes nach der neuen Richtlinie s. unten B. III.

[55] *De lege lata* existiert daher kein sonderrechtlicher Schutz für Algorithmen. Im Rahmen der RL 2009/24/EG des Europäischen Parlaments und des Rates v. 23.4.2009 über den Rechtsschutz von Computerprogrammen, ABl. 2009 L 111, 16 (Computerprogramm-Richtlinie) werden allgemeine Algorithmen gezielt ausgeklammert, vgl. dazu ausführlicher *Triebe*, WRP 2018, 795, 797 mwN. Im Patentrecht wird die Veredelung von Daten mit Hilfe eines Algorithmus ebenfalls im Grundsatz vom Schutz ausgespart (nichttechnischer Natur), vgl. dazu ausführlicher *Färber*, Patentfähigkeit angewandter Algorithmen, 2015, S. 29 ff. mwN. Zusammenfassend *Drexl/Hilty/Desaunettes et al.*, GRUR Int. 2016, 914, 915-916.

[56] Zum Reverse-Engineering von Algorithmen s. unten B. III. 1.

[57] Vgl. zur spiegelverkehrten Algorithm-to-the-data-Methode bereits oben Fn. 50.

[58] Ebenso *Aplin*, in: (Fn. 16), S. 59, 67; zum Verhältnis der Trade-Secrets-Richtlinie zur Computerprogramm-Richtlinie s. die pauschale „unberührt"-Klausel in Erwägungsgrund 39 S. 1 sowie unten B. III. 1.

[59] Vgl. z.B. das Open Source Big Data-Framework *Apache Spark* (https://spark.apache.org); zu Open Source Deep Learning-Algorithmen *Surblyte*, WUW 2017, 120, 123, 126 mwN.

d) Zwischenergebnis

Datensets, Algorithmen, deren Software-Implementierungen und neuronale Netze erfüllen somit in der Regel die Kriterien des kommerziellen Werts und des geheimen Charakters.[60]

3. Angemessene Geheimhaltungsmaßnahmen

Gem. Art. 2 Nr. 1 lit. c muss der potentielle Geheimnisinhaber darüber hinaus den Umständen entsprechende angemessene Geheimhaltungsmaßnahmen treffen. Dieses Kriterium ist zwar international seit geraumer Zeit geläufig,[61] ein Rückgriff auf bestehende Rechtsprechung aus anderen Jurisdiktionen ist allerdings nicht ohne weiteres möglich.[62] Denn die Angemessenheit von Geheimhaltungsmaßnahmen ist in hohem Maße einzelfallabhängig.[63] Aus Art. 11 lässt sich jedenfalls ableiten, dass der Geheimnisinhaber im Hinblick auf die Vornahme angemessener Geheimhaltungsmaßnahmen die Darlegungs- und Beweislast trägt.[64] In der Praxis ist somit eine sorgsame Dokumentation entsprechender Maßnahmen ratsam.[65]

Aus dem Sinn und Zweck der Richtlinie – Innovationsförderung durch Geheimnisschutz – lässt sich ableiten, dass an die Angemessenheit der Maßnahmen keine strengen Anforderungen

---

[60] Über die Kriterien des Art. 2 Nr. 1 hinaus fordern einige Stimmen in der Literatur, dass die jeweiligen Informationen einen Bezug zu einem konkreten Unternehmen aufweisen. Die Richtlinie setze dieses einschränkende Kriterium des „Unternehmensbezugs" implizit voraus, vgl. etwa *Wiese*, in: (Fn. 15), S. 48-50 mwN; a.A. *Hauck*, NJW 2016, 2218, 2221; *Rauer*, GRUR-Prax 2014, 2, 2 (Unternehmensbezug nicht zwingend erforderlich). Wer zugunsten des einschränkenden Kriteriums argumentiert trägt angesichts der klaren Kriterien des Art. 2 Nr. 1 die Argumentationslast. Jedenfalls wird ein Unternehmensbezug bei den hier in Rede stehenden Datensets, Algorithmen und neuronalen Netzen regelmäßig zu bejahen sein. Dieser Bezug ergibt sich bereits daraus, dass die jeweiligen Objekte von dem betreffenden Unternehmen erstellt, genutzt oder gehandelt werden können. Für das regelmäßige Vorliegen eines Unternehmensbezugs allgemeiner *Hauck*, NJW 2016, 2218, 2221.

[61] Vgl. bereits Art. 39 Abs. 2 lit. c TRIPS; vgl. das parallele Kriterium der „reasonable efforts under the circumstances to maintain secrecy" im Trade-Secrets-Recht der USA, s. dazu sowie zu weiteren Gesetzen, in die das Kriterium Eingang gefunden hat *Kalbfus*, GRUR-Prax 2017, 391.

[62] In diese Richtung auch *Kalbfus*, GRUR-Prax 2017, 391, 392; zusammenfassend zur Praxis in den USA und in Japan *Redeker*/*Pres*/*Gittinger*, WRP 2015, 681, 684.

[63] Zur daraus resultierenden Rechtsunsicherheit und der Gefahr unterschiedlicher nationaler Umsetzungen vgl. die im Auftrag der Kommission erarbeitete Studie „Legal Study on Ownership and Access to Data", 2016, S. 10; *Harte-Bavendamm*, in: FS Büscher, 2018, S. 311, 316-320 mwN. Zu denkbaren Kriterien vgl. im Einzelnen *Alexander*, WRP 2017, 1034, 1039 mwN; *Hoeren*/*Münker*, WRP 2018, 150, 152 mwN; *Wiese*, in: (Fn. 15), S. 50-54, 57-59. Die Begründung des RefE geht davon aus, dass Inhalt und Umfang der Geheimhaltungsmaßnahmen von der Art des Geschäftsgeheimnisses im Einzelfall abhängen (S. 20). In der Begründung des RegE wird ergänzt, dass es überdies auf die konkreten Umstände der Nutzung ankomme (S. 22). In Betracht kommen physische Vorkehrungen und vertragliche Sicherungsmechanismen (RefE, S. 20; RegE, S. 22). Der RegE ergänzt, dass es nicht erforderlich sei, jede geheim zu haltende Information gesondert zu kennzeichnen. Vielmehr genüge es grundsätzlich, Maßnahmen für bestimmte Kategorien von Informationen zu ergreifen (bspw. technische Zugangshürden) oder durch allgemeine interne Richtlinien und Anweisung oder auch in Arbeitsverträgen vorzugeben (S. 22). Bei der Wertung der Angemessenheit können insb. folgende Faktoren Berücksichtigung finden: Wert des Geschäftsgeheimnisses, dessen Entwicklungskosten, Bedeutung für das Unternehmen, übliche Geheimhaltungsmaßnahmen in dem Unternehmen, Art der Kennzeichnung der Informationen und vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern. In der Begründung des RegE wird diese Aufzählung um folgende Faktoren ergänzt: Natur der Informationen und Größe des Unternehmens (S. 22). Zur grundsätzlichen Kritik an dieser separaten Schutzvoraussetzung etwa *Lemley*, Stan. L. Rev. 2008, 311, 348-350 mwN (aus Sicht des Trade-Secrets-Rechts der USA).

[64] Vgl. Art. 11 Abs. 1 lit. a, Abs. 2 lit. a, b sowie Köhler/Bornkamm/*Köhler*, Vorbem. §§ 17-19 UWG Rn. 17; vgl. auch die Begründung des RefE, S. 20 sowie des RegE, S. 22.

[65] Denkbar wäre eine Dokumentation im Geheimnisschutzregister vgl. unten Fn. 89.

gestellt werden sollten.[66] Andernfalls könnten Geheimnisinhaber davon absehen, ihre Informationen im Rahmen vernetzter Kooperations- und Wertschöpfungsmodelle miteinander zu teilen.[67] Überdies bestünde die Gefahr, dass Geheimnisinhaber vorsorglich in übertriebene Geheimhaltungsmaßnahmen investieren. Eine strenge Auslegung würde somit ineffizientes Verhalten und erhöhte Transaktionskosten provozieren.[68] Vor diesem Hintergrund sollte es genügen, wenn der Geheimnisinhaber das jeweilige Minimum an Schutzvorkehrungen getroffen hat, das erforderlich ist, um die spezielle Information innerhalb des betreffenden Personenkreises geheim zu halten.[69] In diese Richtung weist auch eine jüngere Entscheidung des österreichischen OGH, die allerdings noch zum autonomen österreichischen Recht erging und die Richtlinie nur am Rande mitberücksichtigt hat.[70] Im zugrundeliegenden Fall hatte der Kläger seine Kundendaten vermeintlich durch ein Passwort geschützt. Aufgrund einer Sicherheitslücke konnte sich die Beklagte jedoch Zugriff verschaffen. Der OGH entschied, dass Sicherheitsmängel dem Geheimnisschutz nicht entgegenstehen, wenn und weil ein „aufrechte[r] Passwortschutz" vorhanden ist. Denn Mitarbeiter und Dritte müssten „[…] redlicherweise annehmen, dass dem Unternehmer diese Mängel nicht bewusst waren, sodass aus deren Vorliegen keinesfalls ein Wegfall des Geheimnischarakters abgeleitet werden kann". Diese Entscheidung spricht somit nicht nur dafür, minimale Geheimhaltungsmaßnahmen ausreichen zu lassen. Geheimhaltungsmaßnahmen können auch dann als angemessen betrachtet werden, wenn sich im Verletzungsfall herausstellen sollte, dass sie überwindbar sind.[71] Voraussetzung ist allein, dass der Geheimnisinhaber subjektiv keine Anhaltspunkte hatte, von einer unzureichenden Sicherung auszugehen und diese innere Tatsache durch das Treffen entsprechender Maßnahmen objektiv erkennbar wurde.[72] Der OGH hat allerdings explizit offengelassen, ob Geheimhaltungsmaßnahmen trotz solcher unbeabsichtigter Sicherheitslücken als angemessene Schutzvorkehrungen i.S.d. Art. 2 Nr. 1 lit. c zu qualifizieren sind und nur

---

66 In diese Richtung auch *Kalbfus*, GRUR-Prax 2017, 391, 392; *Harte-Bavendamm*, in: FS Büscher, 2018, S. 311, 316-321 mwN.

67 Vgl. zur parallelen Argumentation im Hinblick auf den zulässigen Kreis an „Mitwissern" im Bereich Big Data oben B. I. 2. b).

68 Vgl. *Lemley*, Stan. L. Rev. 2008, 311, 313, 334 ff. mwN, der argumentiert, dass ein wesentliches Ziel des Geheimnisschutzes darin liege, (ineffiziente) Investitionen in faktische Geheimhaltungsmaßnahmen zu reduzieren und damit Offenlegung zu fördern: Potentielle Geheimnisinhaber können sich auf den rechtlichen Geheimnisschutz verlassen und sind daher eher bereit, von überzogenen Geheimhaltungsmaßnahmen abzusehen und Informationen zu teilen. Vgl. in diese Richtung auch *Harte-Bavendamm*, in: FS Büscher, 2018, S. 311, 316-321 mwN, der sich dabei auf die allgemeinen Gedanken beruft, die dem Erwägungsgrund 4 S. 4 sowie Erwägungsgrund 9 S. 1 zugrunde liegen.

69 Vgl. in diese Richtung auch *Harte-Bavendamm*, in: FS Büscher, 2018, S. 311, 316-321 mwN; a.A. *Alexander*, WRP 2017, 1034, 1039, der ohne Begründung davon ausgeht, dass ein Minimum an Schutzvorkehrungen nicht genüge. Für die hier vorgeschlagene objektive Betrachtungsweise bei minimalen Anforderungen spricht auch der Zweck des Kriteriums. Es soll die hinreichende Identifizierbarkeit eines Geschäftsgeheimnisses gewährleisten, vgl. dazu *Ohlys* Redebeitrag protokolliert in *Kalbfus/Harte-Bavendamm*, GRUR 2014, 453, 454. Diesem Zweck kann nur durch Zugrundelegung eines hinreichend klar bestimmten Maßstabes Rechnung getragen werden. Legt man stattdessen einen „mittleren" und damit unbestimmten Maßstab an, können Dritte bzw. Arbeitnehmer nicht erkennen, ob ein Geschäftsgeheimnis vorliegt.

70 OGH, Urt. v. 25.10.2016 – 4 Ob 165/16t, BeckRS 2016 117117; vgl. zusammenfassend *Staudegger*, jusIT 2017, 61, 61-62.

71 Vgl. auch *Kalbfus*, GRUR-Prax 2017, 391, 392, der zu Recht darauf verweist, dass der Geheimnisschutz dort einen Hauptanwendungsbereich hat, wo getroffene Schutzvorkehrungen versagt haben.

72 Vgl. *Staudegger*, jusIT 2017, 61, 62.

konstatiert, dass die Mitgliedstaaten einen weitergehenden[73] Schutz von Geschäftsgeheimnissen vorsehen können.[74]

Neben einem Passwortschutz kommen eine Reihe weiterer Geheimhaltungsmaßnahmen in Betracht. Zu denken ist dabei zunächst an Vorkehrungen tatsächlicher und organisatorischer Art, etwa in Gestalt personeller, räumlicher oder technischer Beschränkungen (Verschlüsselung) des Zugangs zu Daten.[75] In rechtlicher Hinsicht können bestehende oder zu begründende Verpflichtungen in Form von arbeitsvertraglichen Verschwiegenheitspflichten und sonstigen Geheimhaltungsvereinbarungen (Non-Disclosure-Agreements, kurz: NDA) als angemessene Geheimhaltungsmaßnahmen qualifiziert werden.[76]

Bei Sachverhalten im Kontext der Datenwirtschaft werden regelmäßig angemessene Geheimhaltungsmaßnahmen im Sinne des Art. 2 Nr. 1 lit. c vorliegen. Denn datenverarbeitende Stellen müssen aus Gründen des Datenschutzes und der IT-Sicherheit ohnehin technisch-organisatorische Schutzmaßnahmen ergreifen.[77]

Hat der Geheimnisinhaber Geheimhaltungsmaßnahmen getroffen, muss er – insbesondere im dynamischen IT-Bereich – fortlaufend überprüfen, ob die getroffenen Schutzvorkehrungen angemessen sind und diese gegebenenfalls anpassen. Andernfalls riskiert er den Verlust seiner Geheimnisse sowohl in faktischer als auch in rechtlicher Hinsicht.[78]

4. Fazit

Zusammenfassend bleibt festzuhalten: Einzeldaten genießen für sich betrachtet keinen Geheimnisschutz. Hierdurch entstehen aber keine ungewollten Schutzlücken. Vielmehr fallen Einzeldaten aus guten Gründen nicht unter den Geheimnisschutz: Sie sind weder schutzwürdig noch schutzbedürftig. An der Schutzwürdigkeit fehlt es, weil Informationen für sich betrachtet möglichst frei von exklusiven Zuordnungen bleiben sollten.[79] An der Schutzbedürftigkeit fehlt es, weil Einzeldaten im Rahmen der Analyse notwendigerweise strukturiert und in Datensets überführt werden müssen. Als deren Bestandteil kommen sie mittelbar in angemessenem Umfang in den Genuss des Geheimnisschutzes. Überdies lassen sich Algorithmen und deren Software-Implementierungen als Geschäftsgeheimnisse qualifizieren. Neuronale Netze genießen in der Regel ebenfalls Geheimnisschutz. Insgesamt sind zwar zwei der drei Schutzvoraussetzungen im Wortlaut der Richtlinie nur schwach konturiert: Erstens das Kriterium des geheimen Charakters, bei dem unklar ist, wie weit der zulässige Kreis von

---

[73] Dem ist allerdings entgegenzuhalten, dass Art. 2 Nr. 1 nach Sinn und Zweck der Richtlinie als vollharmonisierende Norm zu qualifizieren ist, vgl. oben Fn. 14.

[74] Zugunsten einer entsprechenden Auslegung des Art. 2 Nr. 1 lit. c. *Horak*, ecolex 2017, 53, 54; in diese Richtung auch *Alexander*, WRP 2017, 1034, 1039, der allerdings minimale Vorkehrungen nicht genügen lassen will.

[75] Ausführlicher *Aplin*, in: (Fn. 16), S. 59, 67; *Surblyte*, WUW 2017, 120, 125; speziell zu Geschäftsgeheimnissen, die im Internet veröffentlicht wurden oben Fn. 38.

[76] *Sattler*, in: (Fn. 33), S. 27, 38 mwN; speziell zu Verträgen mit Cloud-Anbietern: *Surblyte*, WUW 2017, 120, 125. Soweit es wegen der Besonderheiten von Big Data (Volume, Velocity, vernetzte Wertschöpfungs- und Kooperationsmodelle) im Einzelfall unpraktikabel, unsicher oder gar unmöglich sein sollte, alle Geschäftsgeheimnisse auf vertraglicher Grundlage abzusichern, kann bzw. muss (ergänzend) auf faktische Geheimhaltungsmaßnahmen zurückgegriffen werden, vgl. *Wiebe*, GRUR Int. 2016, 877, 880.

[77] Ausführlicher *Sagstetter*, in: (Fn. 7) mwN (im Erscheinen).

[78] *Alexander*, WRP 2017, 1034, 1038; *Cundiff*, IDEA 2009, 359, 363-364 mwN.

[79] Vgl. allgemein *Dorner*, CR 2014, 617, 621-622; Erwägungsgrund 16 S. 1.

Mitwissern zu ziehen ist. Zweitens das Erfordernis angemessener Geheimhaltungsmaßnahmen, bei dem offenbleibt, welche Maßstäbe gelten und welche konkreten Maßnahmen dem Geheimnisinhaber abverlangt werden. Sinn und Zweck der Richtlinie – Innovationsförderung durch grenzüberschreitenden Geheimnisschutz – sprechen allerdings für eine weite und unionsweit einheitliche Auslegung.[80] Der Geheimnisschutz ist daher bereits *de lege lata* von erheblicher Bedeutung für typische Big Data-Sachverhalte.

II. Schutzsubjekt: Inhaberschaft des Geschäftsgeheimnisses

1. Ausgangspunkt: Vage Legaldefinition

Obwohl die Frage, wem Geschäftsgeheimnisse zugeordnet werden, von zentraler Bedeutung ist, begnügt sich die Richtlinie mit einer vagen Legaldefinition:[81] Inhaber eines Geschäftsgeheimnisses ist nach Art. 2 Nr. 2 jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis besitzt. Damit bleibt insbesondere offen, wem ein Geschäftsgeheimnis zuzuordnen ist, wenn mehrere Personen an dessen Entstehung beteiligt sind.[82] Diese Unklarheit ist im Kontext der Datenwirtschaft besonders problematisch, denn hier sind vernetzte Wertschöpfungsketten besonders häufig und im Interesse der Innovation besonders förderungswürdig.[83] Betrachtet man beispielsweise die Datenerhebung mittels Sensoren – etwa im Rahmen von Industrie 4.0[84] oder Connected Cars – ist unklar, wer die „rechtmäßige Kontrolle" über das Geschäftsgeheimnis in Form der aggregierten Rohdaten besitzt:

- Ist es der Hersteller des Geräts/der Maschine, in welche(s) die Sensoren integriert wurden oder der Hersteller der Sensoren?
- Ist es der Eigentümer/Halter des Geräts/der Maschine?
- Oder ist es der konkrete Nutzer bzw. ein beteiligter Dienstleister?

Werden Datensets, Algorithmen oder neuronale Netze in einer vernetzten Umgebung gespeichert bzw. ausgetauscht – wie es typischerweise im Rahmen von Big Data-Anwendungen

---

[80] Vor diesem Hintergrund sollte die verbleibende Rechtsunsicherheit nicht überbetont werden. Zur teleologischen Auslegung und Rechtsfortbildung durch den EuGH vgl. allgemein *Leistner/Roder*, ZfPW 2016, 129, 133 mwN. Im Kontext der Trade-Secrets-Richtlinie sprechen insb. die Erwägungsgründe 1-4, 8 für die hier vorgeschlagene weite Auslegung. Dagegen allerdings jdf. partiell *Drexl*, JIPITEC 2017, 257, 269, der eine *spin-off*-Theorie andenkt, nach der Daten, die als reines Nebenprodukt entstehen, vom Schutzgegenstand ausgeklammert werden. Hierdurch würden allerdings Abgrenzungsschwierigkeiten und damit unerträgliche Rechtsunsicherheit hervorgerufen. Vgl. gegen die parallele *spin-off*-Theorie im Bereich des *sui generis*-Rechts *Leistner*, in: (Fn. 16), S. 27, 30.

[81] Vgl. zusammenfassend *Aplin*, in: (Fn. 16), S. 59, 69 mwN; zu Konkretisierungsvorschlägen und vereinzelten möglichen Anhaltspunkten in den Erwägungsgründen vgl. *Alexander*, WRP 2017, 1034, 1040-1041 mwN.

[82] Zu den Folgefragen, die sich stellen, wenn feststeht, dass mehrere Beteiligte Inhaber eines Geschäftsgeheimnisses sind vgl. *Alexander*, WRP 2017, 1034, 1040.

[83] Speziell zur Richtlinie *Aplin*, in: (Fn. 16), S. 59, 69. Allgemein zu diesem schutzrechtsübergreifenden Problem *Leistner*, in: (Fn. 16), S. 27, 34-38 (insb. Fn. 25).

[84] Zu den spezifischen Zuordnungsproblemen im Kontext der Industrie 4.0 s. *Müllmann*, WRP 2018, 1177, 1182 mwN.

geschieht – erschwert dies die Zuordnung zusätzlich.[85] In vielen Fällen dürften dabei mehrere Beteiligte gemeinsame Inhaber eines Geschäftsgeheimnisses werden.

Insgesamt führt die vage Regelung der Inhaberschaft in Verbindung mit den Besonderheiten der vernetzten Datenwirtschaft somit zu erheblicher Rechtsunsicherheit für die unmittelbar Beteiligten – aber auch für Dritte, die Zugang zu Datensets und Algorithmen benötigen, um neue Erkenntnisse zu gewinnen.

2. Privatautonome Regelungen und fakultative Registrierung im „Geheimnisschutzregister"

Relative Rechtssicherheit können die Beteiligten nur erzielen, indem sie die Inhaberschaft privatautonom regeln.[86] Dadurch kann das Geschäftsgeheimnis zugleich einzelfallgerecht zugeordnet werden, denn die Beteiligten wissen in der Regel am besten um die Besonderheiten und Bedürfnisse im Rahmen ihrer Rechtsbeziehung. Der Gesetzgeber hat in dieser Hinsicht hingegen ein Informationsdefizit. Versuche, ein allgemeingültiges Konzept zur Ermittlung des „effektiven" Geheimnisinhabers zu entwickeln, dürften daher scheitern. Allerdings lassen sich auch im Rahmen vertraglicher Lösungen Transaktionskosten und Ungleichgewichtslagen – insbesondere in Form von Informationsasymmetrien – nicht vermeiden. Die Entwicklung spezieller Leitfäden, die Bereitstellung spezifischer Standardverträge und/oder die Schaffung vertragsrechtlicher Regelungen dispositiver und/oder zwingender Natur könnte allerdings dazu beitragen, diese Probleme zu reduzieren.[87] Flankierend könnte man ein Geheimnisschutzregister mit fakultativer Eintragungsmöglichkeit etablieren. Der Inhaber eines Geschäftsgeheimnisses müsste bei der Registrierung einen kryptographischen Fingerabdruck

[85] Zur verteilten Netzwerkstruktur im Rahmen typischer Big Data-Anwendungen s. bereits oben Fn. 45.

[86] Vgl. *Knaak/Kur/Hilty*, IIC 2014, 953, 955 (im Folgenden: MPI-Stellungnahme 2014).

[87] Vgl. zur parallelen Diskussion im Hinblick auf das Datenbankherstellerrecht *Leistner*, in: (Fn. 16), S. 27, 38-39 mwN. Vgl. ferner den jüngst publizierten Leitfaden für die gemeinsame Nutzung von Daten des Privatsektors COM(2018) 232 endg., 1-2, 10 ff.; SWD(2018) 125 endg., 6 ff.

seiner geschützten Informationen hinterlegen.[88] Auf dieser Basis ließe sich die Inhaberschaft rechtssicher und transaktionskostensparend dokumentieren, übertragen und lizenzieren.[89]

III. Schutzwirkung

Art. 3 und 4 begründen und begrenzen die Schutzwirkung des Geheimnisschutzes und bilden damit dessen materiellen Kern.[90] An der Spitze dieser Regelungen steht mit Art. 3 eine vollharmonisierende[91] Auflistung rechtmäßiger Handlungen. Erst im Anschluss normiert Art. 4 die einzelnen Verletzungshandlungen. Durch diese Regelungssystematik wird das allgemeine Regel-Ausnahmeverhältnis klargestellt: Es gilt der Grundsatz der Informations(zugangs)freiheit.[92] Beschränkungen sind rechtfertigungsbedürftig und gelten daher nur für bestimmte Formen des Informationserwerbs bzw. der Nutzung oder Offenlegung von Informationen.

1. Grundsatz der Informations(zugangs)freiheit: Rechtmäßiger Erwerb, rechtmäßige Nutzung und Offenlegung, Art. 3

Ausgangspunkt ist die Generalklausel in Art. 3 Abs. 1 lit. d, die ihr spiegelbildliches Gegenstück in Art. 4 Abs. 2 lit. b findet. Danach gilt jeder Erwerb eines Geschäftsgeheimnisses als rechtmäßig, wenn er unter den gegebenen Umständen mit einer seriösen Geschäftspraxis

---

[88] Ein kryptographischer Fingerabdruck ist eine mathematische Prüfsumme (Hashwert), die durch Anwendung einer nicht umkehrbaren Hashfunktion aus einer Datei erzeugt wird. Bei einer kryptographisch geeigneten Hashfunktion ist es praktisch unmöglich, zwei Dateien zu finden, deren Hashwerte identisch sind, vgl. *Bundesamt für Sicherheit in der Informationstechnik*, Grundlagen der elektronischen Signatur, 2006, S. 123. Im Geheimnisschutzregister sollte aus Effizienz-, Sicherheits- und Geheimhaltungsgründen nur der Hashwert, nicht aber der Inhalt des Geheimnisses gespeichert werden. Zur technischen Realisierung vgl. das in der Praxis meist verwendete Time Stamp Protocol (TSP), s. https://www.ietf.org/rfc/rfc3161.txt. Die Etablierung eines entsprechenden Registers bietet sich auch im Bereich des Datenbankschutzes an. Technisch ließe sich ein solches Register auch ohne Intermediäre auf Basis der Distributed-Ledger-Technologie Blockchain in Form eines verteilten, weltweit öffentlich einsehbaren und grundsätzlich nicht veränderbaren Geschäftsgeheimnis-/Datenbank-Registers umsetzen. Da selbst die Hashwerte großer Dateien nur wenig Speicherplatz benötigen, könnten im Register überdies aktualisierte Fassungen bzw. Echtzeitdaten gespeichert werden. Mein Dank gilt *Dr. Oliver Stiemerling* (Öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung und Geschäftsführer ecambria systems GmbH) für die ausführliche Beantwortung meiner Fragen zu den technischen Grundlagen des kryptographischen Zeitstempelmodells und für die weiterführenden Literaturhinweise. Ferner bedanke ich mich bei Klaus Wiedemann (Doktorand und wissenschaftlicher Mitarbeiter am Max-Planck-Institut für Innovation und Wettbewerb), der im Rahmen der Tagung die mögliche Speicherung von Echtzeitdaten angeregt hat. Zu einer unternehmensinternen Software-Lösung vgl. *Halligan/Weyand*, Trade Secret Asset Management 2018, S. 171 ff. i.V.m. 160-170.

[89] Zur Übertragung und Lizenzierung von Geschäftsgeheimnissen vgl. statt vieler *Zech*, GRUR 2015, 1151, 1156 mwN. Darüber hinaus könnten im Geheimnisregister Geheimhaltungsmaßnahmen dokumentiert werden. In Geheimhaltungsvereinbarungen könnte zudem auf den kryptographischen Fingerabdruck verwiesen werden. Dadurch können geheimzuhaltende Informationen konkret bestimmt werden, ohne dass dadurch das Risiko einer Offenlegung erhöht würde – wie etwa bei einer ausführlichen Beschreibung in einem NDA. Dies ist v.a. bei Geheimhaltungsvereinbarungen im Rahmen von Arbeitsverträgen bedeutsam: Wird ein Geschäftsgeheimnis nicht konkret bezeichnet, ist eine pauschale Verpflichtungen zur Geheimhaltung i.S.e. „Catch-All-Klausel" unwirksam, vgl. *Ziegelmayer*, CR 2018, 693, 696 mwN.

[90] Vgl. *Alexander*, WRP 2017, 1034, 1041.

[91] Vgl. Art. 1 Abs. 1 UAbs. 2; s. aber die Öffnungsklausel für mitgliedstaatlich autonome Freistellungen in Art. 3 Abs. 2.

[92] Vgl. auch Erwägungsgründe 19 und 34.

vereinbar ist.[93] Zur Konkretisierung nennt die Richtlinie drei Beispieltatbestände, Art. 3 Abs. 1 lit. a-c. Im Kontext der Datenwirtschaft sind die unabhängige Entdeckung oder Schöpfung und das Reverse Engineering von besonderer Bedeutung.

Art. 3 Abs. 1 lit. a stellt klar, dass unabhängig entdeckte bzw. entwickelte Informationen frei verwendet werden können und bringt damit einen wesentlichen Grundsatz des Geheimnisschutzes zum Ausdruck: Das Geheimnisschutzregime begründet keine Exklusivrechte des jeweiligen Inhabers.[94] Gewendet auf den Kontext der Datenwirtschaft bedeutet dies: Der Inhaber geheimer Daten oder Algorithmen hat kein Recht, den Zugriff jedes beliebigen Dritten zu unterbinden. Allerdings kann er einen weit gefassten Kreis qualifizierter Dritter vom Zugriff auf seine Geschäftsgeheimnisse ausschließen.[95]

Die Richtlinie stellt ferner die innovations-, aber auch imitationsfördernde[96] Rückwärtsanalyse (Reverse Engineering) als „rechtlich zulässiges Mittel zum Erwerb von Informationen" frei.[97] Dementsprechend gelten nach Art. 3 Abs. 1 lit. b das Beobachten, das Untersuchen, der Rückbau und das Testen eines Produkts als rechtmäßig, soweit dieses öffentlich verfügbar gemacht wurde. Gleiches gilt, wenn sich das Produkt im rechtmäßigen Besitz des Handelnden befindet und dieser keiner rechtsgültigen – gemeint ist: vertraglichen – [98] Pflicht zur Beschränkung des Erwerbs des Geschäftsgeheimnisses unterliegt. Die Richtlinie setzt der Freiheit zur vertraglichen Abbedingung des Reverse Engineerings dabei keine Grenzen,[99] wodurch die Harmonisierungswirkung der Richtlinie unterminiert wird.[100]

Im Kontext der Datenwirtschaft stellt sich die Frage, ob Datensets und Algorithmen als „Produkte" i.S.d. Art. 3 Abs. 1 lit. b qualifiziert werden können. Nach allgemeiner Meinung ist jedenfalls Software ein „Produkt" i.d.S.[101] Es ist kein sachlicher Differenzierungsgrund ersichtlich, der es rechtfertigen könnte, einerseits das Reverse Engineering für Software freizustellen, Algorithmen bzw. Datensets insofern aber andererseits absoluten Schutz zu gewähren.[102] Vielmehr spricht der Umstand, dass Software auf Algorithmen und Daten beruht

---

93 S. dazu sowie zur spiegelbildlichen Generalklausel in Art. 4 Abs. 2 lit. b ausführlicher unten B. III. 2. a).

94 Vgl. Erwägungsgrund 16 S. 1; *Alexander*, WRP 2017, 1034, 1041 („grundlegende Aussage"); s. aber *Harte-Bavendamm*, in: FS Köhler, 2014, S. 235, 245 („Selbstverständlichkeit").

95 S. ausführlicher sogleich unten B. III. 2. a) c).

96 Zum Reverse Engineering im Spannungsverhältnis von Innovations- und Imitationswettbewerb *Harte-Bavendamm*, in: FS Köhler, 2014, S. 235, 245-248 mwN; *Ohly*, in: Waldeck/Pyrmont, Patents and technological progress in a globalized world, 2009, S. 535, 536-538, 546 ff. mwN.

97 Vgl. auch Erwägungsgrund 16 S. 3; zur geplanten Umsetzung im § 2 Abs. 2 Nr. 2 des RefE vgl. *Triebe*, WRP 2018, 795, 804 mwN; s. nun § 3 Abs. 1 Nr. 2 des RegE (identischer Wortlaut). In der Begründung des RegE (S. 24) wird nur ergänzt, dass die vertragliche Abbedingung des Reverse Engineering wirksam sein muss.

98 Ebenso *Kalbfus*, GRUR 2016, 1009, 1012 (allerdings einschränkend: „wohl"); *Surblyte*, in: (Rn. 48), S. 725, 744.

99 Vgl. Erwägungsgrund 16 S. 4. Zur Einführung zwingenden Rechts vgl. oben B. II. 2. Häufig werden vertragliche Einschränkungen in AGB enthalten sein. Insoweit ist denkbar, dass die in Art. 3 Abs. 1 lit. b zum Ausdruck kommende grundsätzliche Zulässigkeit der Rückwärtsanalyse nicht pauschal und ohne schutzwürdige Interessen des Geheimnisinhabers abbedungen werden kann, vgl. *Keller*, GRUR 2018, 706, 707; zu sonstigen Grenzen vgl. *Triebe*, WRP 2018, 795, 804 mwN sowie *Wiese*, in: (Fn. 15), S. 124-132, 149 mwN, die überdies für ein pauschales Verbot vertraglicher Beschränkungen des Reverse Engineerings plädiert.

100 Vgl. *Radoń*, Trade Secrets Protection for 'Big Data', 2015, S. 46; für eine genauere Festlegung der vertraglichen Grenzen des Reverse Engineering allgemein *Ohly*, in: (Fn. 96), S. 535, 546.

101 Vgl. *Surblyte*, in: (Fn. 48), S. 725, 739 f.

102 In diese Richtung auch *Radoń*, Trade Secrets Protection for 'Big Data', 2015, S. 47, die sich allerdings nur auf den weiten Wortlaut des Art. 3 Abs. 1 lit. b beruft.

bzw. diese im Rahmen von Softwareanwendungen genutzt oder erzeugt werden, für eine Gleichbehandlung. Dies ist von besonderer Bedeutung, denn das Phänomen Big Data erleichtert es, öffentlich zugängliche oder rechtmäßig erworbene Datensets zu analysieren, zu kombinieren und dadurch Geschäftsgeheimnisse zu rekonstruieren. Praktisch bedeutsam ist dabei vor allem die Rückwärtsanalyse in Form der De-Anonymisierung.[103] Durch Kombination mit anderen Daten lässt sich in einer Vielzahl von Fällen ein Personenbezug (wieder-)herstellen – selbst, wenn die Informationen, die dem Datenset zugrunde liegen, prima facie anonymisiert sind oder keinen Personenbezug aufweisen.[104] Beispielsweise können auf diesem Weg (vermeintlich) anonymisierte Kunden- oder Lieferantenlisten eines Unternehmens entschlüsselt werden. Bezieht man in die Analyse weitere Daten aus öffentlich zugänglichen Quellen[105] mit ein, lassen sich Geschäftsgeheimnisse eines Unternehmens – etwa die aktuelle Geschäftslage[106] oder Herstellungsverfahren – rekonstruieren.[107] Ob der Reverse Engineer die Geschäftsgeheimnisse, die er auf diesem Weg erworben hat, nutzen oder offenlegen darf, ist damit allerdings noch nicht entschieden. Denn dem Wortlaut nach ist die Freigabe der Rückwärtsanalyse auf den „Erwerb" des Geheimnisses beschränkt. Es ist daher umstritten, inwieweit Informationen, die im Rahmen der Rückwärtsanalyse gewonnen wurden, verwendet werden dürfen.[108] Richtigerweise folgt aus dem systematischen Zusammenhang mit Art. 4 Abs. 3, dass im Wege des Reverse Engineerings erworbene Kenntnisse in der Folge auch genutzt und offengelegt werden dürfen.[109] Aus Gründen der Rechtssicherheit wäre neben einer Klarstellung dieser Problematik wünschenswert, dass die Richtlinie das Konkurrenzverhältnis zu entsprechenden Freistellungen in anderen Rechtsgebieten explizit adressiert.[110] So fehlt insbesondere eine Klarstellung des Verhältnisses zur begrenzten Freistellung des Reverse Engineerings in Art. 5 Abs. 3, 6 je i.V.m. Art. 8 Computerprogramm-Richtlinie.

---

[103] Vgl. *Radoń*, Trade Secrets Protection for 'Big Data', 2015, S. 47.

[104] Vgl. statt vieler *Mayer-Schönberger/Cukier*, Big Data, 2017, S. 13 ff. mwN und zahlreichen Beispielen.

[105] Vgl. bereits *Hammerl*, ZIP 1994, 1230, 1231 ff. mwN zum Freedom of Information Act; zum öffentlichen Informationsfreiheitsrecht in Deutschland im Verhältnis zur Trade-Secrets-Richtlinie vgl. *Goldhammer*, NVwZ 2017, 1809 ff. mwN.

[106] Hieraus lässt sich die aktuelle Geschäftsbewertung eines Unternehmens ableiten. Nach *Dorner* wurde ein Unternehmen, das eine auf dieser Idee basierende Wirtschaftsdatenbank anbieten wollte, durch die bisherige autonome deutsche Rechtslage davon abgeschreckt, das entsprechende Projekt in die Tat umzusetzen, vgl. *Dorner*, Vortrag „Die neue Geschäftsgeheimnis-RL (RL 2016/943/EU): Paradigmenwechsel im Know-how-Schutz?" auf dem Symposium „Die neue Geschäftsgeheimnis-Richtlinie" am 13.10.2017 an der Friedrich-Alexander-Universität Erlangen-Nürnberg (im Folgenden: Symposium Geschäftsgeheimnis-Richtlinie).

[107] Vgl. zu weiteren Beispielen *Henseler-Unger*, in: (Fn. 33), S. 1, 19-20.

[108] Vgl. für einen Überblick über den Meinungsstand das Protokoll der Sitzung des Fachausschusses für Wettbewerb und Markenrecht zum insoweit gleichlautenden Richtlinienvorschlag (COM(2013) 813 endg.) *Kalbfus/Harte-Bavendamm*, GRUR 2014, 453, 455.

[109] So bereits *Harte-Bavendamm*, in: FS Köhler, 2014, S. 235, 245 zum systematisch parallelen Art. 3 Nr. 3 des Richtlinienvorschlags; in diese Richtung auch MPI-Stellungnahme 2014, 961; *Wiese*, in: (Fn. 15), S. 126 ff. mwN.

[110] Vgl. dazu *Surblyte*, in: (Fn. 48), S. 725, 745 mwN. Die Begründung des RefE (S. 21) begnügt sich mit einem pauschalen Verweis auf immaterialgüterrechtliche und lauterkeitsrechtliche Schranken, vgl. *Triebe*, WRP 2018, 795, 804 mwN; ebenso die Begründung des RegE (S. 24).

2. Ausnahme: Schutz vor bestimmten Verletzungshandlungen, Art. 4

Art. 4 unterscheidet drei Arten von Verletzungshandlungen, die kaskadenartig aufeinanderfolgen: den Erwerb, die Nutzung und die Offenlegung von Geschäftsgeheimnissen. Art. 4 Abs. 2 und 3 erläutern und konkretisieren diese Verletzungsformen. Art. 4 Abs. 4 und 5 erweitern den Geheimnisschutz im Hinblick auf Verletzungshandlungen Dritter und Verhaltensweisen im Zusammenhang mit rechtsverletzenden Produkten.[111]

a) Konkretisierung der Verletzungsformen in Art. 4 Abs. 2

Im Kontext der Datenwirtschaft ist insbesondere der konkrete Verletzungstatbestand in Art. 4 Abs. 2 lit. a hervorzuheben. Danach ist der Zugang zu, die Aneignung bzw. das Kopieren von elektronischen Daten als rechtswidrig zu qualifizieren, wenn die jeweilige Handlung ohne Zustimmung des Rechtsinhabers erfolgt und kein Rechtfertigungsgrund („unbefugt") greift.[112] Die erlangten Daten müssen das Geschäftsgeheimnis nicht enthalten. Vielmehr genügt es, wenn das Geschäftsgeheimnis aus den erlangten Daten abgeleitet werden kann.

Ergänzt wird dieser konkrete Verletzungstatbestand durch eine sehr weit gefasste Generalklausel in Art. 4 Abs. 2 lit. b, die ihr spiegelbildliches Gegenstück in Art. 3 lit. d findet. Beide Bestimmungen nehmen auf den unbestimmten Rechtsbegriff der „seriösen Geschäftspraktiken" Bezug: Eine Verhaltensweise ist rechtmäßig (rechtswidrig), wenn sie unter den jeweiligen Umständen mit einer „seriösen Geschäftspraxis" (nicht) vereinbar ist. Dabei handelt es sich um einen autonomen Begriff des Unionsrechts, über dessen Auslegung letztlich der EuGH entscheiden muss.[113] Die Öffnungsklauseln in Art. 3 und 4 führen damit auf der einen Seite zu erheblicher Rechtsunsicherheit.[114] Auf der anderen Seite eröffnen sie einen breiten Spielraum für flexible und bereichsspezifische Konkretisierungen.[115] Dies ist gerade im Kontext der Datenwirtschaft bedeutsam, da die technische und wirtschaftliche Entwicklung dort besonders rasant voranschreitet und sehr schwer vorhersehbar ist.

b) Erwerb, Nutzung und Offenlegung durch Dritte, Art. 4 Abs. 4

Art. 4 Abs. 4 gewährt unter zwei Voraussetzungen Geheimnisschutz gegen Verletzungshandlungen Dritter.[116] Objektive Voraussetzung ist, dass der Dritte über eine Person in den Besitz des Geheimnisses gelangt ist, die dieses ihrerseits i.S.d. Art. 4 Abs. 3 rechtswidrig genutzt oder offengelegt hat. In subjektiver Hinsicht ist erforderlich, dass der Dritte um diesen Umstand wusste oder hätte wissen müssen. Maßgeblicher Zeitpunkt ist der Erwerb, die Nutzung oder die Offenlegung des Geheimnisses. Der Geheimnisschutz entfaltet

---

[111] Vgl. dazu im Einzelnen *Alexander*, WRP 2017, 1034, 1042-1043 mwN.

[112] Vgl. hierzu *Alexander*, WRP 2017, 1034, 1042; *Wiese*, in: (Fn. 15), S. 94-95, 102.

[113] Vgl. dazu im Einzelnen Harte-Bavendamm/Henning-Bodewig/*Harte-Bavendamm*, Vor §§ 17-19 UWG Rn. 10c; *Alexander*, WRP 2017, 1034, 1041 mwN; *Wiese*, in: (Fn. 15), S. 96-101 mwN. Denkbar ist allerdings, dass der EuGH den Mitgliedstaaten die nähere Konkretisierung überlässt, vgl. Fn. 130.

[114] Vgl. etwa die Kritik von *Harte-Bavendamm*, in: FS Köhler, 2014, S. 235, 248-249.

[115] Die Öffnungsklauseln können dabei zugleich als Einfallstor für die Berücksichtigung übergeordneter Wertungen dienen, wie sie insbesondere aus der Grundrechtecharta fließen.

[116] Vgl. dazu auch Erwägungsgrund 29 sowie im Einzelnen *Alexander*, WRP 2017, 1034, 1042-1043; *Grassie*, JIPLP 8 (2014), 677, 680 mit Beispielen.

somit Ausschlusswirkung gegenüber jedem bösgläubigen Dritten. Die Richtlinie verschärft dabei die Drittwirkung, indem sie den Maßstab der Bösgläubigkeit im Vergleich zur bisherigen deutschen Rechtslage bzw. Art. 39 Abs. 2 TRIPS auf einfache Fahrlässigkeit absenkt.[117] Die Rechtsposition des Geheimnisinhabers wird somit insoweit stärker „verdinglicht"[118]. Über den genauen Grad der „Verdinglichung" wird jedoch letztlich der EuGH entscheiden.[119] Je stärker die Anforderungen an das Kennenmüssen dabei abgesenkt werden, desto näher rückt der Geheimnisschutz auf der Skala der „Verdinglichung" an die absoluten Schutzrechte.[120]

c) Rechtsverletzende Produkte, Art. 4 Abs. 5

Partielle Ausschlusswirkung gegenüber Dritten entfaltet auch Art. 4 Abs. 5. Danach kann der Geheimnisinhaber unter anderem das Herstellen, Anbieten oder Inverkehrbringen von Produkten verbieten, die auf seinen Geschäftsgeheimnissen beruhen.[121] In objektiver Hinsicht muss allerdings eine Erheblichkeitsschwelle überschritten sein, ehe das Produkt als „rechtsverletzend" zu qualifizieren ist. Dies ist erst dann der Fall, wenn Konzeption, Merkmale, Funktionsweise, Herstellungsprozess oder Marketing des Produkts in erheblichem Umfang auf den rechtswidrig erworbenen, genutzten oder offengelegten Geschäftsgeheimnissen beruhen.[122] Subjektive Voraussetzung ist, dass der Handelnde von der rechtswidrigen Nutzung i.S.d. Art. 4 Abs. 3 wusste oder hätte wissen müssen.

Datensets und Algorithmen, die im Rahmen des Art. 4 Abs. 5 aus fremden Geschäftsgeheimnissen abgeleitet wurden, können als „Produkte" i.S.d. Art. 2 Nr. 4 qualifiziert werden. Dafür spricht neben dem Wortlaut die entsprechende Auslegung des gleichlautenden Begriffs in Art. 3 Abs. 1 lit. b.[123] Ob sich überdies auch Dienstleistungen unter Art. 4 Abs. 5 fassen lassen, bleibt unklar.[124] Der ohnehin breite Anwendungsbereich des Art. 4 Abs. 5 würde dadurch jedenfalls noch weiter ausgedehnt.[125] Dem ist durch restriktive Auslegung der objektiven und subjektiven Voraussetzungen Rechnung zu tragen. Andernfalls droht Art. 4 Abs. 5 über die Ziele der Richtlinie hinauszuschießen – sie sogar zu konterkarieren. Denn je ungewisser und höher das Risiko, dass Waren, die im Zusammenhang mit fremden Informationen entwickelt wurden, als rechtsverletzende Produkte zu qualifizieren sind, desto

---

[117] *Hoeren/Münker*, CCZ 2018, 85, 86 mwN; a.A. *Wiese*, in: (Fn. 15), S. 116-118. Kritisch auch *Brammsen*, BB 2018, 2446, 2450 der die Fahrlässigkeitshaftung bei mittelbaren Rechtsverletzungen als „gänzlich inakzeptabel" bezeichnet und ein daraus resultierendes „Informationseigentum erga omnes" ablehnt. Zur grundsätzlich gelungenen Abstimmung des Geheimnisschutzes mit der Informationsfreiheit s. aber oben III. 1 sowie unten C.

[118] Grundlegend zur Verdinglichung im Grenzbereich von Schuld- und Sachenrecht: *Dulckeit*, Die Verdinglichung obligatorischer Rechte, 1951; *Canaris*, in: FS Flume, Bd. 1, 1978, S. 371 ff. Kritisch zu Elementen der Verdinglichung im Rahmen des Know-how-Schutzes *Dorner*, Know-how-Schutz im Umbruch, S. 117 ff. mwN.

[119] Vgl. aber Fn. 130.

[120] Gegen eine allgemeine Nachforschungspflicht *Alexander*, WRP 2017, 1034, 1042-1043; *Wiese*, in: (Fn. 15), S. 147.

[121] Speziell zur Haftung Dritter *Hoeren/Münker*, CCZ 2018, 85, 86 mwN.

[122] Vgl. die Legaldefinition in Art. 2 Nr. 4.

[123] S. oben B. III. 1.

[124] Befürwortend MPI-Stellungnahme 2018, S. 9.

[125] Zur Kritik an der weiten Fassung des Art. 4 Abs. 5 i.V.m. Art. 2 Nr. 4 und weiteren offenen Fragen vgl. statt vieler MPI-Stellungnahme 2014, S. 957-958.

eher werden Unternehmen davon absehen, fremde – und gegebenenfalls sogar objektiv freie – Informationen als Ausgangspunkt für eigene Innovationen zu nutzen.[126]

3. Fazit

Auf der Skala der Schutzwirkung steht der Geheimnisschutz somit zwischen reinen Marktverhaltensregelungen und vollständigen Ausschließlichkeitsrechten wie dem Patent.[127] Die Richtlinie verstärkt den Grad der Verdinglichung und rückt den Geheimnisschutz damit näher an die absoluten Schutzrechte. So schützt sie den Geheimnisinhaber zwar weiterhin nicht gegen den Zugriff beliebiger Dritter, weist ihm aber Ausschließlichkeitsrechte gegen einen weit gefassten Kreis qualifizierter Dritter zu, vgl. Art. 4 Abs. 4 und 5. Ein Blick auf die Rechtsfolgenseite bestätigt diesen Befund: Art. 12, 14 und 15 gewähren dem Geheimnisinhaber Ansprüche auf Schadensersatz[128], Unterlassung und die Möglichkeit, Gerichtsentscheidungen zu veröffentlichen. Die Rechtsbehelfe der Trade-Secrets-Richtlinie sind damit an diejenigen der Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums angenähert.[129] Einschränkend ist allerdings zu berücksichtigen, dass die Trade-Secrets-Richtlinie eine signifikant höhere Anzahl dezidierter Verhältnismäßigkeitsschranken enthält.[130]

Der neue Geheimnisschutz entfaltet vor diesem Hintergrund eine robuste negative Ausschlusswirkung. Der positive Zuweisungsgehalt ist allerdings schwächer ausgestaltet: Im Interesse von Innovation und Wettbewerbsförderung bleiben unabhängige Entdeckungen und Rückwärtsanalysen freigestellt.[131]

4. Ausnahmen

Art. 5 enthält einen Katalog besonderer Situationen, in denen der Geheimnisschutz im Einzelfall hinter andere schützenswerte Interessen zurücktreten kann.[132] Erforderlich ist stets eine konkrete Interessenabwägung im Einzelfall. Im Kontext der Datenwirtschaft ist namentlich Art. 5 lit. a von Bedeutung. Danach muss sich der Geheimnisschutz stets einer Abwägung mit

---

[126] Die Begründung des RegE (S. 31) versucht diesem Umstand auf Rechtsfolgenebene Rechnung zu tragen, indem der Anspruch auf Rückruf oder Vernichtung aufgrund Unverhältnismäßigkeit ausgeschlossen wird, wenn die Produkte nur deshalb als rechtsverletzend qualifiziert werden, weil sie Gegenstand eines rechtswidrigen Marketings sind.

[127] So zu Recht vor dem Hintergrund des deutschen Rechts: *Ohly*, GRUR 2014, 1, 3; vor dem Hintergrund der Richtlinie ähnlich *Wiese*, in: (Fn. 15), S. 146-147 mwN. In diese Richtung nun auch die Begründung des RefE (S. 16, 22); ebenso die Begründung des RegE (S. 17, 25). Ausführlicher zur Rechtsnatur des Geheimnisschutzes *Niebel*, in: FS Fezer, 2016, S. 799, 802 ff. mwN; im Lichte des RefE für eine Einordnung als Immaterialgüterrecht *Kiefer*, WRP 2018, 910 ff. mwN.

[128] Dazu ausführlich *Böhm/Nestler*, GRUR-Prax 2018, 181 ff. mwN.

[129] Vgl. dazu *Hofmann*, WRP 2018, 1, 3; *Gärtner/Goßler*, MittPatAnw 2018, 204, 206; zur den daraus resultierenden Haftungsrisiken für Wettbewerber vgl. *Ziegelmayer*, CR 2018, 693, 698.

[130] Der Grad der Verdinglichung wird somit gerade im Bereich der Rechtsdurchsetzung davon abhängen, wie der EuGH mit diesem flexibleren Rechtsrahmen umgehen wird – sei es, dass er selbst unmittelbare Entscheidungen trifft oder die Konkretisierung (in gewissen Grenzen) den mitgliedstaatlichen Gerichten überlässt.

[131] Diese Freistellungen sind allerdings auch im Urheberrecht geläufig: unabhängige Doppelschöpfung, begrenzt zulässiges Reverse Engineering im Softwarebereich, vgl. *Ohly*, GRUR 2014, 1, 3; zum Zuweisungsgehalt des Geheimnisschutzes *Zech*, GRUR 2015, 1151, 1156.

[132] Ausführlicher *Alexander*, WRP 2017, 1034, 1043-1044 mwN.

der grundrechtlich verbürgten Meinungs-, Medien- und Informationsfreiheit stellen.[133] Sonstige legitime Interessen, die auf nationaler oder unionsrechtlicher Ebene anerkannt sind, können über die Auffangklausel in Art. 5 lit. d Berücksichtigung finden. Aus dem systematischen Zusammenhang folgt allerdings, dass derartige Interessen mit den in Art. 5 lit. a bis c genannten Fällen vergleichbar sein müssen.[134] Art. 5 dient damit als Einfallstor für die Berücksichtigung übergeordneter Wertungen – wie sie insbesondere aus der Grundrechtecharta fließen. Dadurch provoziert die Richtlinie zwar erneut erhebliche Rechtsunsicherheit, eröffnet aber zugleich einen breiten Spielraum für flexible und bereichsspezifische Konkretisierungen.[135] Es bedarf weiterer Forschung, ob darüber hinaus konkrete sektorspezifische Zugangs-, Nutzungs- und flankierende Informationsrechte etabliert werden sollten, um den freien Datenfluss im Interesse der Innovation und des Wettbewerbs zu fördern.[136] Gerade im Bereich des Geheimnisschutzes sind zusätzliche spezielle Freistellungen allerdings besonderes rechtfertigungsbedürftig, weil Geheimhaltung und Informationsunvollständigkeiten in gewissen Grenzen sogar innovations- und wettbewerbsfördernd wirken können.[137] Jedenfalls wäre hier ein tauglicher Ankerpunkt für die Schaffung begrenzter Zugangs- und Informationsrechte im Hinblick auf Algorithmen.[138] Auf diesem Weg ließe sich das – möglicherweise sogar grund- und menschenrechtlich gebotene – Ziel erreichen, algorithmenbasierte Entscheidungen transparent(er) zu machen.[139] Insgesamt sollte jeweils flankierend ein Recht auf Auskunft über die jeweiligen Metadaten etabliert werden. Denn eines der Hauptprobleme der derzeitigen Datenmärkte liegt im Informationsdefizit über Herkunft, Erhebungsmethode sowie Aktualität und damit über die Qualität der Daten.[140]

---

[133] Ausführlicher *Wiese*, in: (Fn. 15), S. 132-133 mwN; *Alexander*, WRP 2017, 1034, 1044 mwN.

[134] So zu Recht *Alexander*, WRP 2017, 1034, 1044.

[135] Vgl. zur besonderen Bedeutung eines flexiblen Rechtsrahmens für die dynamische datengetriebene Wirtschaft oben B. III. 2. a).

[136] Zum Abbau ungerechtfertigter Beschränkungen des freien Datenflusses und der Notwendigkeit, Zugang zu Daten für öffentliche und private Akteure sicherzustellen vgl. statt vieler *Leistner*, in: (Fn. 16), S. 27, 42 ff. mwN sowie die Mitteilungen der Kommission oben Fn. 6.

[137] Vgl. hierzu *Leistner*, in: (Fn. 16), S. 27, 45 (insb. Fn. 45); allgemeiner *Drexl*, NZKart 2017, 339. Vgl. auch den Vortrag von *Ohly* „Know-how-Schutz und Patentrecht" auf dem Symposium Geschäftsgeheimnis-Richtlinie: Geschützter Raum der Vertraulichkeit („Laborzone") als Voraussetzung funktionierenden Wettbewerbs (Tagungsbericht *Kurz/Magnus*, WRP 2018, 126, 127).

[138] Vgl. dazu *Radoń*, Trade Secrets Protection for 'Big Data', 2015, S. 59 mwN.

[139] Insb. könnte der Mensch durch die Anwendung intransparenter Algorithmen zum Objekt degradiert werden, vgl. *Martini*, JZ 2017, 1017 ff. mwN. Zur Offenlegung von Algorithmen i.R.d. Verordnung 2016/679/EU des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. 2016 L 119, 1 (Datenschutz-Grundverordnung) vgl. den Beitrag von *Lars Rühlicke* in diesem Tagungsband mwN. Zur Offenlegung von Algorithmen im Kontext neuronaler Netze *Erbguth*, DRiZ 2018, 130, 131; differenzierend *Bues*, in: Hartung/Bues/Halbleib, Legal Tech – Die Digitalisierung des Rechtsmarkts, 2018, S. 275, 283 mwN.

[140] Vgl. allgemein zu dem Problem der mangelnden Offenlegung, auf welche Art und Weise Daten gesammelt (Herkunft, Qualität), organisiert und analysiert (Methodik) werden und zu den daraus resultierenden besonderen Problemen im Bereich Big Data: *Mattioli*, BTJL 2017, 1-51; *Hoeren*, MMR 2016, 8, 11.

C. Fazit und Ausblick

Neben dem Datenbank-[141] und Datenschutz ist der Geheimnisschutz die dritte wesentliche Säule des „Europäischen Datenrechts".[142] Seine herausragende Bedeutung für die Datenwirtschaft[143] folgt im Ausgangspunkt daraus, dass Datensets, Algorithmen und neuronale Netze regelmäßig unter die weite Definition des Geschäftsgeheimnisses fallen. Durch differenzierte teleologische Auslegung der einzelnen Kriterien lässt sich kompensieren, dass die Belange der Datenwirtschaft bei Schaffung der Richtlinie nicht bedacht und breite Anleihen beim TRIPS-Abkommen aus den neunziger Jahren genommen wurden. Aus Gründen der Rechtssicherheit und Rechtsklarheit sollten in die Richtlinie bzw. die nationalen Umsetzungsakte allerdings entsprechende Klarstellungen aufgenommen werden.[144]

Mit der neuen Trade-Secrets-Richtlinie erfährt die Schutzwirkung des Geheimnisschutzes überdies eine erhebliche Aufwertung. Der Inhaber eines Geschäftsgeheimnisses kann sich nun auf eine robuste Ausschlusswirkung gegenüber einem weit gefassten Kreis qualifizierter Dritter verlassen. Im Interesse von Informationsfreiheit, Innovation und Wettbewerbsförderung sichert die Richtlinie andererseits wichtige Freiräume.[145]

Die Verwendung einer Vielzahl unbestimmter Rechtsbegriffe und die einzelfallbezogene Verhältnismäßigkeitsprüfung auf Durchsetzungsebene eröffnet dabei gerade im Bereich Big Data einen breiten Spielraum für flexible Konkretisierungen. Zugleich resultiert daraus allerdings erhebliche Rechtsunsicherheit. Der genaue Umfang des Geheimnisschutzes im Kontext der Datenwirtschaft wird daher erst durch die mitgliedstaatlichen Gerichte bzw. den EuGH konturiert werden.[146] Wegen des differenzierenden Harmonisierungskonzepts drohen dabei in wichtigen Bereichen erheblich divergierende nationale Geheimnisschutzregime zu entstehen, denen die Richtlinie gerade abhelfen wollte.[147] Besonders problematisch ist dies bei der – wie oben gezeigt – notwendigerweise vagen Legaldefinition des Geheimnisinhabers.

---

[141] Zur Rolle des Datenbankurheber- und Datenbankherstellerrechts im Kontext von Big Data samt entsprechenden Reformvorschlägen *Leistner*, in: (Fn. 16), S. 27 ff. mwN; *Sagstetter*, in: (Fn. 7) (im Erscheinen).

[142] Zur Bedeutung des Datenbank- und Geheimnisschutzes für die Datenwirtschaft *de lege lata* sowie *de lege ferenda Sagstetter*, in: (Fn. 7) (im Erscheinen).

[143] Zur herausragenden Bedeutung des Geheimnisschutzes für digitale Geschäftsmodelle vgl. auch *Dorner*, Vortrag auf dem Symposium Geschäftsgeheimnis-Richtlinie (Tagungsbericht *Kurz/Magnus*, WRP 2018, 126, 127).

[144] Zwar werden i.R.d. RefE und des RegE „Unternehmensdaten" als Beispiel für Geschäftsgeheimnisse genannt (RefE, S. 19; RegE, S. 22). Zu Recht weist das MPI in seiner Stellungnahme zum RefE aber darauf hin, dass es sich dabei nicht um einen *Terminus technicus* handelt und damit weiterhin Rechtsunsicherheit herrscht, vgl. MPI-Stellungnahme 2018, S. 6. Der Terminus ist überdies vor dem Hintergrund der zahlreichen Anknüpfungspunkte in Big Data-Konstellationen zu undifferenziert, vgl. dazu B. I. 2.

[145] *Aplin*, in: (Fn. 16), S. 59, 70; a.A.: *Zech*, JIPITEC 2015, 192, 197 „[…] protection is incomplete […]".

[146] Vgl. Fn. 130.

[147] Kritisch zur Konzeption der Trade-Secrets-Richtlinie als teils mindestharmonisierendem Instrument etwa auch *Falce*, IIC 2015, 940 ff. Hier könnten die nach Art. 17 einzurichtenden Korrespondenzstellen eine wichtige Rolle spielen, indem sie die jeweilige mitgliedstaatliche Rechtsprechung dokumentieren und damit eine Abstimmung zwischen den Mitgliedstaaten erleichtern. Darüber hinaus wäre zu überlegen, den Korrespondenzstellen weitere Aufgaben zu übertragen, die zur Harmonisierung und Rechtssicherheit beitragen.

Rechtssicherheit können die Beteiligten nur erzielen, indem sie vertragliche Vorkehrungen treffen. Flankierend sollte ein Geheimnisschutzregister etabliert werden. Mit dessen Hilfe ließe sich das Geschäftsgeheimnis rechtssicher und transaktionskostensparend dokumentieren, lizenzieren und übertragen. Im Übrigen bedarf es weiterer Forschung, ob die Schaffung sektorspezifischer zwingender Zugangs-, Nutzungs- und Informationsrechte erforderlich ist.

Bei entsprechender Optimierung ist das neue Geheimnisschutzregime in der Lage, den Anforderungen der Datenwirtschaft adäquat Rechnung zu tragen.[148] Im Verbund mit einem optimierten Datenbank- und Datenschutzrecht kann der Geheimnisschutz den bestehenden *acquis communautaire* so ergänzen, dass im Kontext von Big Data-Sachverhalten weder Überschutz gewährt wird noch unbeabsichtigte Schutzlücken bleiben.[149]

Die faktische Herrschaft über die Daten ergänzt durch vertragliche Gestaltungen genügt zumindest aus zwei Gründen nicht als alleinige Basis der Datenwirtschaft: erstens sind zahlreiche Unternehmen zu Vertraulichkeitsvereinbarungen nicht bereit;[150] zweitens fehlt dem Vertragsrecht die Drittwirkung[151] des Art. 4 Abs. 4, 5. Ein robuster gesetzlicher Geheimnisschutz bietet dadurch einen zusätzlichen Anreiz für das Teilen von Daten und trägt damit zur Durchbrechung faktischer Datenmonopole bei. Hierfür ist es allerdings notwendig, das genaue Verhältnis des Geheimnisschutzes zu sonstigen Schutzinstrumenten rechtlicher und faktischer Art zu bestimmen.[152] Denn eine unkoordinierte Schutzrechtskumulation birgt die Gefahr, dass die Wertungen des Geheimnisschutzes bzw. anderer Schutzinstrumente konterkariert werden.[153]

Darüber hinaus ist zu bedenken, dass Daten, Algorithmen und neuronale Netze nicht an den europäischen Außengrenzen Halt machen. Eine weitergehende internationale Vereinheitlichung des Geheimnisschutzes wäre daher in theoretischer Hinsicht wünschenswert.[154] Geheimnisbegriff und Struktur der Verletzungshandlungen sind jedenfalls

---

[148] In diese Richtung auch *Drexl*, JIPITEC 2017, 257, 269, der vertritt, dass der begrenzte Schutzansatz der Richtlinie (Zugangsschutz) jedenfalls besser geeignet ist, den Bedürfnissen der Datenwirtschaft Rechnung zu tragen als die Einführung eines Exklusivrechts an Daten.

[149] In diese Richtung auch *Aplin*, in: (Fn. 16), S. 59, 72 mwN; a.A. *Zech*, GRUR 2015, 1151, 1156: „Geheimnisschutz als unzureichender Rechtsrahmen".

[150] Vgl. dazu sowie zum Arrowschen Informationsparadoxon *Lemley*, Stan. L. Rev. 2008, 311, 336-337; zur Entlastungsfunktion des dispositiven Rechts allgemein *Behrens*, Die ökonomischen Grundlagen des Rechts, 1986, S. 157-158; *Fleischer*, Informationsasymmetrie im Vertragsrecht, 2001, S. 181-182; *Unberath/Cziupka*, AcP 2009, 37, 50-51.

[151] S. aber zu „ausschließlichkeitsähnlichen" Bindungen durch vertragliche Konstruktionen in Kombination mit tatsächlichen Schutzmaßnahmen *Specht*, CR 2016, 288, 289-290 mwN.

[152] Hierauf kann im Rahmen des Beitrags aus Platzgründen nicht näher eingegangen werden. Vgl. zum Verhältnis von Geheimnis- und Datenschutz Erwägungsgründe 34 und 35; *Radoń*, Trade Secrets Protection for 'Big Data', 2015, S. 48-53 mwN; *Malgieri*, IDPL 2016, 102 ff. mwN (Auflösung des Spannungsverhältnisses mittels „De-Kontextualisierung"; *Sagstetter*, in: (Fn. 7) (im Erscheinen); zum Verhältnis von Geheimnis- und Datenbankschutz vgl. Erwägungsgrund 39 S. 1; SWD(2018) 147 endg., 43-44 sowie die unterstützende Studie des Joint Institute for Innovation Policy (JIIP) im Auftrag der Kommission, 2018, S. 88-91. Zum Verhältnis von lauterkeitsrechtlichem Leistungs- und Geheimnisschutz vgl. *Becker*, GRUR 2017, 346, 347 ff., 355.

[153] Allgemein zu den Problemen, die aus sich überlagernden Schutzinstrumenten resultieren: *Derclaye/Leistner*, Intellectual property overlaps, 2011; *Leistner*, Konsolidierung und Entwicklungsperspektive des Europäischen Urheberrechts, 2008, S. 50 ff.

[154] In diese Richtung auch *Surblyte*, in: (Fn. 48), S. 725, 736; zu bisherigen Modellvorhaben vgl. MüKo-Lauterkeitsrecht/*Brammsen*, Vorbem. §§ 17-19 UWG, Rn. 12-13.

international anschlussfähig.[155] So finden sich die auf Art. 39 Abs. 2 TRIPS zurückgehenden Begrifflichkeiten und entsprechende Strukturen in einer Vielzahl von Rechtsordnungen, insbesondere im Trade-Secrets-Recht der USA[156].[157]

Ganz i.S.d. Tagungstitels bleibt damit festzuhalten: Das neue Recht des Geheimnisschutzes stellt eine flexible, international anschlussfähige und – bei entsprechender Optimierung – ausgewogene Infrastruktur für (datengetriebene) Innovation bereit.

---

[155] Vgl. zu den Begrifflichkeiten *Goldhammer*, NVwZ 2017, 1809 mwN.

[156] Vgl. *Ferrari*, Big Data – Balancing the Web User's and the Service Provider's Rights in the Big Data Era, 2017, S. 116-118 mwN.

[157] S. statt vieler insb. Art. 9 des revidierten Wettbewerbs- und Kartellrechts der Volksrepublik China v. 4.11.2017 (Geltung seit 1.1.2018, zu den starken Ähnlichkeiten mit der Richtlinie bzw. dem Trade-Secrets-Recht der USA vgl. die Zusammenfassung der neuen Regelung bei: https://www.cliffordchance.com/briefings/2018/03/17th_global_ip_newsletter.html, S. 12-13); speziell zu dem Erfordernis angemessener Geheimhaltungsmaßnahmen s. den rechtsvergleichenden Überblick bei *Kalbfus*, GRUR-Prax 2017, 391, 391-392. In Japan wurde jüngst eine partielle Revision des Unfair Competition Prevention Acts beschlossen, um einen Anreiz für die (gemeinsame) Datennutzung zu schaffen, vgl. dazu ausführlicher http://www.meti.go.jp/english/policy/economy/chizai/chiteki/index.html; http://www.meti.go.jp/english/press/2018/0907_003.html; https://aippi.org/no-show/partial-revision-of-the-unfair-competition-prevention-act/. Der revidierte Rechtsakt etabliert ab dem 1.7.2019 ein separates Schutzregime für qualifizierte Daten ohne geheimen Charakter („Protected Data"). Zur bisherigen Rechtslage in Japan vgl. *Matuso*, in: Jager, Trade Secrets throughout the World, 2017, Bd. 2, S. 358, 360 ff. mwN.