Digitaler Strukturwandel und Privatrecht

– Neue Regeln für Big Data & Co.? *

*Thomas Sagstetter***

* Dieser Beitrag basiert auf einem Vortrag, den der Verfasser iRd 29. Jahrestagung der Gesellschaft Junger Zivilrechtsrechtswissenschaftler an der Ruhr-Universität Bochum gehalten hat. Die Tagung stand unter dem Generalthema „Strukturwandel und Privatrecht“. Der Beitrag wird demnächst im entsprechenden Tagungsband veröffentlicht. Die Open-Access-Vorabveröffentlichung erfolgt mit freundlicher Genehmigung des NOMOS Verlages. Literatur konnte bis Ende Januar 2019 berücksichtigt werden.

** 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. Für weiterführende Hinweise und Gespräche danke ich überdies *Lucie Antoine, Prof. Dr. Ansgar Ohly, LL.M. (Cambridge), Dr. Lars Rühlicke, Dr. Andreas Sattler, LL.M. (Nottingham), Dr. Oliver Stiemerling* und den Mitgliedern der Forschungsgruppe „Datengetriebene Wirtschaft: Regulierungsbedarf infolge von Digitalisierung“ am Max-Planck-Institut für Innovation und Wettbewerb in München.

A. Einführung

Der Diskussion um die Regulierung der Datenwirtschaft liegt in unterschiedlichem Umfang die Ausgangsprämisse zugrunde, der aktuelle Rechtsrahmen biete keine (adäquate) Infrastruktur für den digitalen Strukturwandel in Gestalt von Big Data & Co.[1] Vor diesem Hintergrund werden in Teilen der Literatur eigenständige, eigentumsähnliche Rechte an Daten postuliert und konstruiert.[2] Zwar spricht sich die überwiegende Meinung in der europäischen Literatur mittlerweile gegen die Schaffung neuer Rechte an Daten aus.[3] Die Kommission hat die Idee, neue Rechte an Daten einzuführen, aber noch nicht explizit *ad acta* gelegt.[4] Überdies hat die europäische Diskussion entsprechende Debatten in zahlreichen Drittstaaten angestoßen.[5]

---

1 Eine allgemeingültige Definition des Begriffs Big Data existiert nicht. Es handelt sich dabei um einen schillernden Sammelbegriff, der regelmäßig als Schlagwort für den Umgang mit großen und heterogenen Datenmengen unter Einsatz von Algorithmen im Rahmen unterschiedlicher Kontexte genutzt wird. Vgl ausführlich zum schillernden Begriff Big Data *Schütze*/*Hänold*/*Forgó*, Big Data – Eine informationsrechtliche Annäherung, in Kolany-Raiser/Heil/Orwat et al. (Hg) Big Data und Gesellschaft – Eine multidisziplinäre Annäherung (Wiesbaden 2018) 233 (234, 237-238 mwN). Für den Sammelbegriff „Datenwirtschaft" (vgl etwa SWD(2018) 146 endg, 2: „von Maschinen erzeugte Daten, IoT-Geräte, Big Data, KI usw") gelten diese Ausführungen entsprechend. Auch für die einzelnen Technologien, die im Rahmen typischer Big Data-Sachverhalte verwendet werden, existiert keine allgemeingültige Definition, vgl etwa zu dem Begriff Künstlicher Intelligenz (KI) *Bues*, Artificial Intelligence im Recht, in Hartung/Bues/Halbleib (Hg) Legal Tech – Die Digitalisierung des Rechtsmarkts (München 2018) 275 (276-279 mwN). Wesentliches Charakteristikum typischer Big Data-Sachverhalte und der damit verbundenen Phänomene ist jedenfalls der verfolgte Zweck: Durch die Analyse großer Datenmengen sollen neue Erkenntnisse gewonnen werden, die in Ansehung einzelner Datensätze verborgen geblieben wären. In diese Richtung (allerdings nur für das Phänomen Big Data) *Fries*, PayPal Law und Legal Tech – Was macht die Digitalisierung mit dem Privatrecht?, NJW 2016, 2860 (2862 Fn 28). Für die juristische Bewertung ist eine konturscharfe Definition entbehrlich, wenn sich die verschiedenen Phasen eines typischen Big Data-Sachverhalts herauskristallisieren lassen, vgl dazu unten B. I. sowie *Schütze*/*Hänold*/*Forgó*, Big Data – Eine informationsrechtliche Annäherung (Fn 1) 233 (238).

2 Die Diskussion in Europa wurde maßgeblich gefördert durch die Äußerungen des damals zuständigen EU-Kommissars *Günther Oettinger* im April 2015: „Wir brauchen ein virtuelles und digitales Sachenrecht, das auch für Daten gilt.", vgl dazu *Drexl*, Neue Regeln für die Europäische Datenwirtschaft?, NZKart 2017, 339 (340 Fn 7 mwN). Zu den verschiedenen Konstruktionsversuchen *de lege lata* sowie den Vorschlägen *de lege ferenda* vgl den Überblick bei *Duisberg*, „Datenhoheit und Recht des Datenbankherstellers" – Recht am Einzeldatum vs. Rechte an Datensammlungen, in Smart-Data-Begleitforschung (Hg) Daten als Wirtschaftsgut (Backnang 2017) 16 (19-24 mwN); *Specht*, Rechtsvergleichende Analyse des zivilrechtlichen Umgangs mit Daten in den Rechtsordnungen Deutschlands und der USA, in ABIDA (Hg) Datenrechte – eine Rechts- und Sozialwissenschaftliche Analyse im Vergleich Deutschland – USA (Münster 2017) 9 (69-80 mwN). Für die Einführung eines Immaterialgüterrechts *sui generis* des Einzelnen an seinen verhaltensgenerierten Daten *Fezer*, Theorie des immaterialgüterrechtlichen Eigentums an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten, MMR 2017, 3 ff; *ders*, Repräsentatives Dateneigentum – Ein zivilgesellschaftliches Bürgerrecht (Berlin 2018); zu einem parallelen – allerdings explizit eigentumsrechtlich basierten – Ansatz vgl jüngst *Amstutz*, Dateneigentum, AcP 218 (2018), 438 (479 ff mwN). Zur Kritik an beiden Ansätzen unten Fn 158. Zum Begriff „Dateneigentum"/„data ownership" vgl *Specht,* Rechtsvergleichende Analyse (Fn 2) 9 mwN.

3 Vgl *Dreier* in Dreier/Schulze UrhG (2018) Vorbemerkung §§ 87a ff Rn 15 mwN.

4 Vgl nur SWD(2017) 304 endg Teil 1/2, 2-3: „[…] 'ownership' rights […] on non-personal data […] and liability, are more difficult topics and less mature topics that deserve further assessment.". Für die Einführung eines Ausschließlichkeitsrechts an Daten in der Literatur bspw jüngst wieder *Tjong Tjin Tai*, Data ownership and consumer protection, EuCML 2018, 136 ff; *Amstutz*, AcP 218 (2018), 438 (483 ff, 521 ff).

5 Zur Diskussion in den USA vgl *Mayer*/*Ritter*, Regulating Data as Property: A new construct for moving forward, Duke L & Tech Rev 2018, 220 (223 ff, 262 ff mwN); *Mattioli* plädiert für die Einführung eines „*datarights*", das ein ausschließliches Nutzungsrecht an Daten einräumt, wenn die Methoden ihrer Erhebung, Verarbeitung sowie ihre Kontextualisierung offengelegt werden. Ziel dieses Ansatzes ist es, die Qualität der Daten und ihrer Analyse sicherzustellen bzw zu erhöhen s *Mattioli*, Disclosing Big Data, Minn L Rev 2014, 535 (578 ff). Allerdings gibt es in den USA bislang überraschenderweise keine politische Diskussion, die mit der europäischen vergleichbar wäre, vgl

Wer neue Schutzrechte fordert, setzt sich allerdings dem Vorwurf aus, den zweiten vor dem ersten Schritt zu tun. Denn es ist fraglich, ob die Ausgangsprämisse zutrifft: Bietet der bestehende Rechtsrahmen wirklich keine angemessene Infrastruktur für Big Data & Co.?

Zur Beantwortung dieser Frage ist zunächst zu klären, inwieweit die neuen Phänomene im Kontext der Datenwirtschaft einen Strukturwandel ausgelöst haben. Die schillernden Begriffe verleiten dazu, von einem tiefgreifenden Strukturwandel auszugehen. Im Kern handelt es sich allerdings bei all diesen Phänomenen weiterhin um elektronische Datenverarbeitung (EDV) unter Anwendung mathematisch-statistischer Verfahren.[6] Ein Strukturwandel lässt sich nur in zweierlei Hinsicht feststellen: Zum einen werden die Analysewerkzeuge durch die Weiterentwicklung (selbstlernender) Algorithmen samt entsprechender Infrastruktur immer leistungsfähiger und erleichtern eine automatisierte Auswertung.[7] Zum anderen wächst die Menge an maschinenlesbaren und damit algorithmisch analysierbaren Informationen exponentiell. Letztlich beobachten wir damit bei nüchterner Betrachtung nur die fortschreitende Weiterentwicklung der Informations- und Wissensgesellschaft – Evolution statt Revolution.[8] Das Privatrecht versucht dem damit einhergehenden digitalen Strukturwandel schon seit Jahrzehnten Rechnung zu tragen, indem es Informationen, Daten(banken) und Algorithmen schützt oder bewusst freistellt.

Vor diesem Hintergrund liegt die Vermutung nahe, dass das Privatrecht keiner Revolution, sondern allenfalls einer gezielten Reform bedarf. Der Beitrag wird diese Vermutung bestätigen: Namentlich das *sui generis*-Recht nach der europäischen Datenbank-Richtlinie[9] sowie das

---

Kerber, Rechte an Daten in der digitalen Ökonomie: Analyse öffentlicher Diskussionsprozesse und der in ihnen verwendeten Argumentation, in ABIDA (Hg) Datenrechte – eine Rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA (Münster 2017) 115 (192-197 mwN); *Specht,* Rechtsvergleichende Analyse (Fn 2) 9 (80-83 mwN); zur Diskussion in China vgl SWD(2018) 147 endg, 39; zur Diskussion in Japan *Mayer*/*Ritter*, Duke L & Tech Rev 2018, 220 (222, 232-240, 246 mwN); zur Einführung eines separaten Schutzregimes für qualifizierte Daten ohne geheimen Charakter („Protected Data") in Japan *Sagstetter*, Big Data und der europäische Rechtsrahmen: Status quo und Reformbedarf im Lichte der Trade-Secrets-Richtlinie 2016/943/EU in Maute/Mackenrodt (Hg) Recht als Infrastruktur für Innovation (Baden-Baden 2019) 285 (317 Fn 157 mwN).

6 In diese Richtung für KI auch *Jordan*, Artificial Intelligence – The Revolution Hasn't Happened Yet, 4.5.2018, abrufbar unter https://rise.cs.berkeley.edu/blog/michael-i-jordan-artificial-intelligence%E2%80%8A-%E2%80%8Athe-revolution-hasnt-happened-yet/ [Alle Internetquellen wurden zuletzt am 31.10.2018 abgerufen]; vgl auch *Bues*, Artificial Intelligence (Fn 1) 275 (275 ff): *Bues* verweist zum einen darauf, dass bereits seit den fünfziger Jahren an KI geforscht wird. Zum anderen stellt er klar, dass die „Intelligenz" im Rahmen des *Machine Learnings* (ML) auf Wahrscheinlichkeit und Statistik beruht. Vgl auch *Herberger*, „Künstliche Intelligenz" und Recht, NJW 2018, 2825 (2826), der zu Recht für eine nüchterne Einschätzung plädiert.

7 Zur automatisierten Datenanalyse etwa bereits BVerfG NJW 1984, 419 (422) – Volkszählungsurteil „[...] unter den Bedingungen der automatischen Datenverarbeitung [gibt es] kein „belangloses" Datum mehr." Durch die neuen Analysetechniken können freilich Erkenntnisse gewonnen werden, die mit herkömmlichen Mitteln nicht oder allenfalls unter Einsatz eines wesentlich höheren (Zeit-)Aufwands hätten erlangt werden können, vgl dazu *Dorner*, Big Data und „Dateneigentum", CR 2014, 617 (617).

8 Zur Informations- und Wissensgesellschaft als Selbstbeschreibung der Moderne ausführlich *Zillien*, Digitale Ungleichheit (Wiesbaden 2009) 5 ff mwN.

9 Richtlinie 96/9/EG über den rechtlichen Schutz von Datenbanken v 11.3.1996, ABl 1996 L 77, 20 (Datenbank-Richtlinie; im Folgenden: DB-RL). Auf die Bedeutung des Datenbankurheberrechts nach Art 3 DB-RL kann aus Platzgründen nicht eingegangen werden, vgl dazu *Leistner*, Big Data and the EU Database Directive 96/9/EC, in Lohsse/Schulze/Staudenmayer (Hg) Trading data in the digital economy: legal concepts and tools (Baden-Baden 2017) 27 (51 f).

Geheimnisschutzregime nach der Trade-Secrets-Richtlinie[10] stellen eine Infrastruktur für Big Data & Co. bereit, indem sie Informationen, Daten(banken) bzw. (selbstlernenden) Algorithmen einerseits weitreichenden Schutz gewähren und andererseits bewusst wichtige Freiräume sichern.[11]

Es erstaunt, dass dies bislang nicht hinreichend berücksichtigt wurde, stehen doch die Besonderheiten und Belange der datengetriebenen Wirtschaft im Zentrum europäischer Rechtssetzungs-, Revisions- und Evaluationsbemühungen.[12]

So wurde die Datenbank-Richtlinie jüngst ein zweites Mal evaluiert – mit einem besonderen Fokus auf das *sui generis*-Recht und dessen Bedeutung für die Datenwirtschaft.[13] Die Kommission kam dabei allerdings zu dem zweifelhaften Ergebnis, dass das Datenbankherstellerrecht „im Großen und Ganzen nicht für die Datenwirtschaft" gelte.[14]

Die Bedeutung des Geheimnisschutzes für die datengetriebene Wirtschaft wurde bereits im Rahmen der Rechtssetzung unterschätzt.[15] Diese Fehleinschätzung setzt sich bis heute fort.[16]

Vor diesem Hintergrund ist es notwendig, die Bedeutung des Datenbank- und Geheimnisschutzes für die Datenwirtschaft gezielt zu analysieren. Dabei ist in einem ersten Schritt zu untersuchen, wie weit der Datenbank- und Geheimnisschutz in typischen Sachverhalten im Kontext der Datenwirtschaft bereits *de lege lata* reicht. In einem zweiten Schritt ist jeweils *de lege ferenda* die Frage aufzuwerfen, welche Änderungen erforderlich sind, um den Datenbank- bzw. Geheimnisschutz

---

[10] Richtlinie 2016/943/EU über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung v 8.6.2016, ABl 2016 L 157, 1 (Trade-Secrets-Richtlinie; im Folgenden: TS-RL).

[11] Die Relevanz des Datenbank- bzw Geheimnisschutzes für die Datenwirtschaft wurde bislang nur vereinzelt und jeweils isoliert untersucht, vgl für den Datenbankschutz *Leistner*, Big Data (Fn 9) 27-57; für den Geheimnisschutz *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285-318.

[12] 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 je mwN. Zusammenfassend *Czychowski/Siesmayer* in Kilian/Heussen (Hg) Computerrechts-Handbuch (34. Aufl. München 2018) Teil 20.5 (Rn. 1). 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*, Free Flow of Data?, IIC 2018, 397 (397 ff mwN).

[13] SWD(2018) 147 endg; zusammenfassend SWD(2018) 146 endg; s auch die begleitende Studie des Joint Institute for Innovation Policy (JIIP) im Auftrag der Kommission (im Folgenden: *JIIP*, Study) samt begleitenden Materialien unter https://ec.europa.eu/digital-single-market/en/news/study-support-evaluation-database-directive.

[14] S SWD(2018) 146 endg, 2; ausführlicher SWD(2018) 147 endg, 35-37, 47 mwN und zahlreichen „Angstklauseln", in denen jeweils betont wird, dass die Bedeutung des *sui generis*-Rechts im Rahmen der künftigen Datenwirtschaft genau geprüft werden muss. Zurückhaltender *JIIP*, Study (Fn 13) 20, 78, 111-115: „In the data economy context, it means that most machine-generated data should remain out of the scope of the sui generis right, though it is not always clear whether the data is generated (created) rather than obtained (collected)." In diese Richtung bereits COM(2017) 9 endg, 11 ff, in der die Kommission davon ausging, dass von Maschinen erzeugte Rohdaten für sich genommen idR keinen Datenbank- oder Geheimnisschutz genießen, s zum Schutz von Einzeldaten B. I. 2. a), B. I. 3. a) sowie B. I. 4.

[15] Dazu *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (285 ff mwN).

[16] Vgl zum Umsetzungsprozess in Deutschland in Gestalt des Referenten- und Regierungsentwurfs *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (287 ff mwN). Die endgültige Fassung des Umsetzungsgesetzes [Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) v 18.4.2019, BGBl I 2019 466] zielt ebenso wenig wie der Referenten- und Regierungsentwurf bzw. die Richtlinie darauf ab, den Besonderheiten und Bedürfnissen der Datenwirtschaft gerecht zu werden. Vgl zu den im Kontext dieses Beitrags relevanten Änderungen im Vergleich zu den Entwürfen unten Fn 43, 44, 141.

an den begrenzten Strukturwandel in Gestalt von Big Data & Co. – exponentielles Wachstum der verfügbaren Daten sowie neue Analysewerkzeuge – anzupassen.

Die Analyse der beiden Schutzregime fügt sich in den eingangs skizzierten allgemeineren Rahmen: Lässt sich der bestehende Rechtsrahmen an die Besonderheiten und Bedürfnisse der Datenwirtschaft anpassen, entfällt bereits im Ausgangspunkt jede Rechtfertigung für die Einführung neuer Schutzinstrumente.[17]

B. Die Relevanz des Datenbank- und Geheimnisschutzes für die europäische Datenwirtschaft de lege lata und de lege ferenda

I. Schutzgegenstand

Im Rahmen typischer Big Data-Sachverhalte bieten sich im Ausgangspunkt zahlreiche Bezugspunkte für einen rechtlichen Schutz an. Dem trägt die bisherige Diskussion um die Regulierung der Datenwirtschaft nicht angemessen Rechnung. Denn sie fokussiert sich bis heute auf Rechte an „Daten“[18]. Damit wird die Diskussion in zweierlei Hinsicht unzulässig verkürzt.

Erstens sind Daten divers.[19] So sind mindestens drei Kategorien von Daten zu unterscheiden:

- Einzeldaten,
- Datensets (strukturiert bzw. unstrukturiert),[20]
- Metadaten[21].

Zweitens basiert das Phänomen Big Data nicht nur auf großen Datenmengen. Erst die (selbstlernenden) Algorithmen [22] in Verbindung mit der entsprechenden Infrastruktur

---

17 Vgl *Aplin*, Trading Data in the Digital Economy: Trade Secrets Perspective, in Lohsse/Schulze/Staudenmayer (Hg) Trading data in the digital economy: legal concepts and tools (Baden-Baden 2017) 59, 72 sowie C.

18 Zu den schillernden (Rechts-)Begriffen „Daten“ und „Informationen“ vgl statt vieler *Zech*, Information als Schutzgegenstand (Tübingen 2012) 32 ff; *Specht,* Rechtsvergleichende Analyse (Fn 2) 9 (12-14, 214 f); *Determann*, No one owns data, Hastings Law Journal 2018 1 (6 f mwN). Zur theoretischen Abgrenzung zwischen Zeichen- bzw Bedeutungsebene vgl *Drexl*, NZKart 2017, 339 (343 mwN); *Wiebe*/*Schur*, Ein Recht an industriellen Daten im verfassungsrechtlichen Spannungsverhältnis zwischen Eigentumsschutz, Wettbewerbs- und Informationsfreiheit, ZUM 2017, 461 (469 f, 472): Der Schutz auf syntaktischer Ebene bewirkt jedenfalls mittelbar auch den Schutz der dahinterliegenden Informationen auf semantischer Ebene. Umgekehrt betrifft eine Regulierung auf semantischer Ebene idR auch die syntaktische Ebene. *Amstutz* plädiert für einen alternativen medientheoretischen Datenbegriff, der dezidiert vom Daten-Inhalt losgelöst ist: *Amstutz*, AcP 218 (2018), 438 (448 ff).

19 Vgl allgemein zur Vielfalt an Daten *Becker*, Rechte an Industrial Data und die DSM-Strategie, GRUR Newsletter 01/2016, 1 (7); *Duisberg,* „Datenhoheit und Recht des Datenbankherstellers“ (Fn 2) 16 (23 mwN).

20 Hier kann theoretisch weiter nach personen- und nicht personenbezogenen Datensets differenziert werden, vgl hierzu sowie zu dem Begriff der Kommunikationsdaten ausführlicher ab Fn 169.

21 Zur Abgrenzung von Primär- und Metadaten *Krüger*/*Möllers*, Metadaten in Justiz und Verwaltung, MMR 2016, 728 mwN*;* zur Rolle der Metadaten bei der Datenkontextualisierung *Amstutz*, AcP 218 (2018), 438 (467 mwN).

22 Zur Definition des Begriffs Algorithmus vgl *Drexl*/*Hilty*/*Desaunettes et al*, Ausschließlichkeits- und Zugangsrechte an Daten, GRUR Int 2016, 914 (916); *Busch*, Algorithmic Accountability (Münster 2018) 9 ff mwN; zur technologischen und wirtschaftlichen Bedeutung von Algorithmen vgl *Scheja*, Schutz von Algorithmen in Big Data Anwendungen, CR 2018, 485, (485-486 mwN). Zu selbstlernenden Algorithmen vgl. *Amstutz*, AcP 218 (2018), 438 (504-508 mwN).

(Rechenleistung und Übertragungsgeschwindigkeit)[23] machen große Datenmengen wertvoll. Denn aus Massendaten lassen sich nur mithilfe von Algorithmen neue Erkenntnisse ableiten. Die Daten müssen in der Regel zunächst durch Algorithmen verifiziert, kontextualisiert und strukturiert werden.[24] Im Anschluss können sie – wiederum durch Algorithmen – analysiert werden.

Angesichts dessen ist in zwei Schritten vorzugehen, um alle relevanten Rechtsobjekte zu identifizieren: Zunächst ist der typische Big Data-Prozess zu sezieren. In einem zweiten Schritt ist zu untersuchen, ob die – dadurch sichtbar gewordenen – einzelnen Bestandteile schutzwürdig und schutzbedürftig sind.

1. Potenziell relevante Rechtsobjekte in typischen Big Data-Sachverhalten

Der typische Big Data-Prozess lässt sich in drei kaskadenartig aufeinanderfolgende Phasen unterteilen:[25] Datenbeschaffung, Datenanalyse und Umgang mit den Ergebnissen der Analyse.

a) Erste Phase: Datenbeschaffung (ggf. inkl. Datenvalidierung)

Das Ausgangsmaterial einer Big Data-Analyse („originäre Daten“) wird extern auf dem Datenmarkt[26] und/oder aus frei zugänglichen Quellen beschafft und/oder selbst erhoben. Bei der Datenerhebung ist zwischen maschinengenerierten und von Personen erfassten Daten zu unterscheiden: Ein maschinengeneriertes Datum entsteht, sobald ein Sensor einen bestimmten Wert ausgibt (Beispiel: ‚3‘ [Volt]).[27] Ein solches „Einzeldatum“[28] (Sensordatum ‚3‘) hat allerdings keine Aussagekraft.[29] Einen Informationsgehalt erlangt das Einzeldatum erst, wenn es durch Metadaten kontextualisiert wird.[30] Die Metadaten beziehen sich dabei zunächst nur auf das Einzeldatum und ordnen ihm Bestimmungsmerkmale zu (Beispiel: Einheit [Grad], Ort und Zeit der Messung, Messparameter, etc.). Hierdurch entsteht ein „Datenset“ (Beispiel: 30 Grad am 11.9.2018 um 13 Uhr). Gegebenenfalls

---

[23] Vgl zur besonderen Bedeutung der Infrastruktur im Rahmen der Datenwirtschaft *Becker*, GRUR Newsletter 01/2016, 1 (7).

[24] Vgl zur notwendigen Strukturierung von Daten *Bundeskartellamt*/*Autorité de la Concurrence*, Competition Law and Data (Bonn 2016) 6 mwN; zur notwendigen Strukturierung im Rahmen des Datenaustauschs *Grützmacher*, Dateneigentum – ein Flickenteppich, CR 2016, 485 (487 f mwN). Zur Notwendigkeit der Kontextualisierung ausführlicher sogleich B. I. 1. a), b); zu selbstlernenden Algorithmen in diesem Kontext vgl *Amstutz*, Dateneigentum, AcP 218 (2018), 438 (504-508 mwN).

[25] Vgl *Schütze*/*Hänold*/*Forgó*, Big Data – Eine informationsrechtliche Annäherung (Fn 1) 233 (238). Zur Visualisierung vgl https://www.jura.uni-muenchen.de/personen/s/sagstetter_thomas/vortraege/wem-gehoeren-daten.pdf, Folie 3.

[26] Ausführlich zur Funktionsweise der Datenmärkte *Peitz*/*Schweitzer*, Ein neuer europäischer Ordnungsrahmen für Datenmärkte?, NJW 2018, 275 (275 ff mwN).

[27] Dazu ausführlicher *Amstutz*, AcP 218 (2018), 438 (467 mwN). Eine – ggf integrierte – Software wandelt diesen Wert in eine bestimmte Einheit um. Dabei ist beispielsweise der Faktor 10 vorgegeben, dh der Wert ‚3‘ [Volt] wird zu ‚30‘ [Grad] umgewandelt, vgl dazu das Beispiel bei *JIIP*, Study (Fn 13), 110 (Sensor-generated data in cars).

[28] Teils wird auch die Bezeichnung „Datenpunkt“ verwendet, vgl bspw *Duisberg,* „Datenhoheit und Recht des Datenbankherstellers“ (Fn 2) 16 (17).

[29] Ibid.

[30] Die Kontextualisierung kann bereits unmittelbar nach der Messung erfolgen, indem die bei der Messung anfallenden Metadaten (zB Einheit, Ort und Zeit der Messung, Messparameter) im Anschluss mit dem Sensordatum verknüpft werden.

filtert ein (selbstlernender) Algorithmus bereits an dieser Stelle Messwerte aus, die nicht in die erwartete Messreihe passen oder allgemein nicht den Erwartungen entsprechen („Ausreißer"). Auf diese Art und Weise werden eine Vielzahl von Datensets gesammelt, die sich in ihrer Gesamtheit zunächst als „Datenhaufen" oder „unstrukturierte Datensets" bezeichnen lassen.[31]

Werden Daten von Personen erhoben gelten diese Ausführungen im Grundsatz entsprechend. Im Unterschied zu reinen Sachdaten fehlt es allerdings bereits per definitionem an einem „personenbezogenen" Datum, wenn und soweit das jeweilige Einzeldatum (z.B. Vorname) nicht hinreichend kontextualisiert ist.[32] Im Übrigen wird menschliche Aktivität entweder ebenfalls durch Sensoren erfasst (z.B. Körpertemperatur) oder die Nutzer erstellen die personenbezogenen Daten selbst (z.B. Nutzung von Websites [Tracking-Systeme], Erstellen von Nutzerkonten, Gebrauch vernetzter Gegenstände usw.).[33]

b) Zweite Phase: Datenanalyse (ggf. inkl. Datenvalidierung)

In der Regel werden die einzelnen Datensets unmittelbar nach der Datenerhebung durch (selbstlernende) Algorithmen verarbeitet und in ein strukturiertes Datenset überführt.[34] Dabei werden die einzelnen Datensets in unterschiedliche Kontexte gesetzt, wobei wiederum Metadaten entstehen. Diese Metadaten beschreiben nun nicht mehr die Bestimmungsmerkmale des Einzeldatums, sondern das Verhältnis, in dem die einzelnen Datensets zueinander stehen.[35] Im Rahmen dieses Prozesses entsteht ein „strukturiertes Datenset" bzw. eine „Datenbank". Erst aus diesen strukturierten Datensets lassen sich nun mit Hilfe von (selbstlernenden) Algorithmen neue Erkenntnisse ableiten, die in Ansehung einzelner Daten nicht zu vermuten wären.[36] Werden diese Datensets zum *Text-* und *Data-*

---

[31] Vgl *Peschel*/*Rockstroh*, Big Data in der Industrie, MMR 2014, 571; *Wiebe*, Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, GRUR 2017, 338 (340 mwN); *Zech*, Information as property, JIPITEC 2015, 192 (194).

[32] Vgl Art 4 Nr 1 der Verordnung 2016/679/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG v 27.4.2016, ABl 2016 L 119, 1 (Datenschutz-Grundverordnung; im Folgenden: DSGVO). Danach sind nur solche Informationen als „personenbezogene Daten" zu qualifizieren, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Ohne Kontextualisierung ist eine Identifizierung allerdings unmöglich.

[33] Ausführlicher zu den Erhebungsmöglichkeiten personenbezogener Daten *Bundeskartellamt*/*Autorité de la Concurrence*, Competition Law and Data (Bonn 2016) 6 f mwN; *Kerber*, Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection, GRUR Int 2016, 639 mwN; *Amstutz*, AcP 218 (2018), 438 (502 Fn 358).

[34] Vgl *Wiebe*, GRUR 2017, 338 (342), der darauf hinweist, dass Daten idR nach der Erhebung in einer Datenbank gespeichert werden; *Peschel/Rockstroh*, MMR 2014, 571. Im Rahmen dieser Phase können erneut Validierungsprozesse erfolgen.

[35] Vgl dazu *Duisberg,* „Datenhoheit und Recht des Datenbankherstellers" (Fn 2) 16 (17).

[36] S dazu statt vieler *Fries*, NJW 2016, 2860 (2862 Fn 28) sowie *Mayer-Schönberger*/*Cukier*, Big Data (München 2017) 13 ff; zur notwendigen Strukturierung s bereits Fn 24 mwN.

Mining[37] oder zum Training *Künstlicher Intelligenz* (maschinelles Lernen)[38] genutzt, lassen sie sich als *Korpora*[39] bezeichnen.

(Selbstlernende) Algorithmen analysieren die validierten, kontextualisierten und strukturierten Datensets – insbesondere indem sie die einzelnen Datensets miteinander vergleichen, kombinieren und nach Mustern suchen.

c) Dritte Phase: Umgang mit den Ergebnissen der Analyse (inkl. Präsentation)

Die neuen Erkenntnisse, die im Rahmen der zweiten Phase aus den jeweiligen strukturierten Datensets abgeleitet werden konnten, sind in der Regel ihrerseits als strukturierte Datensets zu qualifizieren, wie beispielsweise das prognostizierte Kaufverhalten bestimmter Kundengruppen („derivative Daten“). [40] Zum Abschluss muss ein Algorithmus bzw. dessen Software-Implementierung die Ergebnisse präsentieren oder die Datensets jedenfalls möglichst so darstellen, dass sich daraus durch menschliche Unterstützung neue Erkenntnisse ableiten lassen.

2. Geheimnisschutz in typischen Big Data-Sachverhalten

Die in den einzelnen Phasen genutzten bzw. geschaffenen unterschiedlichen Arten von Daten, Algorithmen und neuronalen Netzen sind möglicherweise als Geschäftsgeheimnisse im Sinne der Trade-Secrets-Richtlinie zu qualifizieren. [41] Dreh- und Angelpunkt ist die Legaldefinition des Geschäftsgeheimnisses in Art. 2 Nr. 1 TS-RL, die sich eng an Art. 39 Abs. 2 TRIPS anlehnt.[42] 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,[43]

---

[37] Zum Begriff des *Text-* und *Data-Minings* und dessen Bedeutung für Big Data-Analysen sowie einer Zusammenfassung der Rechtslage *Raue*, Das Urheberrecht der digitalen Wissen(schaft)sgesellschaft, GRUR 2017, 11 (13 mwN); *Obergfell,* Big Data und Urheberrecht in Ahrens (Hg) Festschrift für Wolfgang Büscher (Köln 2018) 223 (225 ff mwN).

[38] Zu den technischen Grundlagen des maschinellen Lernens sehr gut verständlich *Stiemerling*, CR 2015, 762 (762 ff); speziell zur KI am Beispiel neuronaler Netze *Ehinger*/*Stiemerling*, Die urheberrechtliche Schutzfähigkeit von Künstlicher Intelligenz am Beispiel von Neuronalen Netzen, CR 2018, 761 (761 ff).

[39] Vgl zu Begriff und Bedeutung der *Korpora Truyens*/*Eecke*, Legal Aspects of Text Mining, Computer Law & Security Review 2014, 153 (154 ff mwN). Im Kontext des maschinellen Lernens lassen sich die Korpora in Trainings- und Testdatensätze unterteilen, die jeweils aus Eingangswerten und den korrekten (dh gewünschten) Ausgangswerten bestehen, vgl *Ehinger*/*Stiemerling*, CR 2018, 761 (762).

[40] Vgl dazu die konkreten Beispiele bei *Mayer-Schönberger*/*Cukier*, Big Data (Fn 36) 71 ff mwN.

[41] Dazu bereits ausführlich *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (290 ff mwN).

[42] Vgl dazu *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (288-290).

[43] Die deutsche Fassung der TS-RL 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 Trade-Secrets-Richtlinie (München 2018) 3 f. Die

- 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.

Diese dreiteilige[44] Definition des Schutzgegenstandes ist – bereits ihrem Wortlaut nach – weit gefasst. Überdies folgt aus Erwägungsgrund 14 TS-RL, dass der Trade-Secrets-Richtlinie ein weiter, technologieneutraler Geheimnisbegriff zugrunde zu legen ist.[45]

a) Einzeldatum

Allerdings erschweren es die Kriterien des „kommerziellen Werts" und des „geheimen Charakters" bereits im Ausgangspunkt, einzelne Daten als Geschäftsgeheimnis zu qualifizieren. Zwar ist das Erfordernis des kommerziellen Werts denkbar weit zu verstehen.[46] Ein nicht kontextualisiertes Einzeldatum – beispielsweise der isolierte Messwert ‚3' ohne Metadaten – hat jedoch für sich genommen keinen potenziell kommerziellen Wert.[47] Kommerziellen Wert erlangen isolierte Einzeldaten – wie oben dargelegt – erst durch Aggregation und/oder Kombination mit Kontextinformationen. Überdies sind kontextlose Einzeldaten als „belanglose Information" zu qualifizieren und damit nach Erwägungsgrund 14 S. 5 TS-RL explizit vom Schutzbereich des Geheimnisschutzes ausgenommen.[48]

b) Datensets

Einzeldaten müssen allerdings im Rahmen typischer Big Data-Sachverhalte notwendigerweise kontextualisiert, strukturiert und in ein Datenset überführt werden.[49] Denn erst aus einem Datenset

fehlerhafte Übersetzung wurde in die endgültige Fassung des deutschen Umsetzungsgesetzes übernommen, vgl § 2 Nr 1 lit a GeschGehG.

44 § 2 Nr. 1 lit c GeschGehG verlangt über den Richtlinientext hinausgehend ein „berechtigtes Interesse an der Geheimhaltung". Sinn und Zweck der Richtlinie – Innovationsförderung durch grenzüberschreitenden Geheimnisschutz – sprechen allerdings für eine unionsweit einheitliche Definition des zentralen Begriffs des „Geschäftsgeheimnisses". Art. 2 Nr 1 TS-RL sollte daher als vollharmonisierende Legaldefinition verstanden werden, vgl dazu ausführlich *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (288 Fn 14 mwN). Vor diesem Hintergrund ist dem unionsrechtswidrigen Kriterium des „berechtigten Interesses" bei der Ausgangsfrage, ob überhaupt eine dem Geheimnisschutz unterliegende Information vorliegt, keine einschränkende Bedeutung beizumessen. Vgl zu den Anforderungen an eine richtlinienkonforme Umsetzung in diesem Kontext bereits das Gutachten der Unterabteilung Europa (PE6), abrufbar unter https://www.bundestag.de/resource/blob/628192/23bfc89c0c4ffb15489850b0558ce23f/PE-6-020-19-pdf-data.pdf mwN.

45 Ausführlich hierzu *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (289-290 mwN).

46 Vgl insb Erwägungsgrund 14 S 3 TS-RL; insgesamt hierzu Fn 45.

47 In diese Richtung auch *Aplin,* Trade Secrets Perspective (Fn 17) 59 (66); für die Qualifikation eines einzelnen Datums als Geschäftsgeheimnis ohne Begründung aber *Scheja*, CR 2018, 485 (489).

48 Ausführlicher hierzu mit weiteren Argumenten gegen einen Geheimnisschutz von Einzeldaten *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (291 f).

49 Vgl Fn 24.

lassen sich mithilfe von Algorithmen potenziell Erkenntnisse ableiten, die in Ansehung einzelner Daten nicht zu vermuten wären.

aa) Kommerzieller Wert

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 fehlt, ist nach allen denkbaren Bemessungsmethoden (markt-, investitions- und prospektivschadenszentriert) ein potenziell kommerzieller Wert eines jeden Datensets zu bejahen.[50]

Ob dem Datenset unstrukturierte Rohdaten („Datenhaufen") oder strukturierte Daten zugrunde liegen, ist unerheblich, weil sich selbst aus unstrukturierten Rohdaten ein – wenn auch geringer – potenziell kommerzieller Wert gewinnen lässt.[51] 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 – wie oben dargelegt – neue Erkenntnisse ableiten und damit potenziell kommerzieller Wert schöpfen. Vor diesem Hintergrund kommt es nicht darauf an, ob das Datenset neben nichtpersonenbezogenen Daten auch solche mit Personenbezug enthält.[52]

Als Zwischenergebnis bleibt somit festzuhalten: Originäre Datensets (strukturiert und unstrukturiert) sind regelmäßig von potenziell kommerziellem Wert. Gleiches gilt für neue Informationen, die aus den Datensets abgeleitet wurden (derivative Daten).

bb) Ausschluss belangloser Informationen

Datensets könnten allenfalls als „belanglose Informationen" vom Schutzbereich ausgeschlossen sein. Allerdings lassen sich aus einem Datenset mithilfe von Algorithmen vielfach belangvolle Erkenntnisse ableiten – selbst wenn es für sich genommen nur belanglose Informationen enthält.[53] Daher kommt – bei der aus teleologischer Perspektive gebotenen Gesamtbetrachtung – der Ausschluss eines Datensets als „belanglose Information" nur in absoluten Ausnahmefällen in Betracht.[54]

cc) Geheimer Charakter

Hinsichtlich des geheimen Charakters lautet die maßgebliche Frage, ob das Datenset in seiner Gesamtheit oder genauen Anordnung und Zusammensetzung allgemein bekannt oder ohne Weiteres

---

[50] Hierzu insgesamt sowie zur regelmäßig vorliegenden Verbindung zwischen kommerziellem Wert und geheimem Charakter *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (289 ff mwN).

[51] *Zech*, A legal framework for a data economy in the European Digital Single Market: rights to use data, JIPLP 2016, 460 (465); *Alexander*, Gegenstand, Inhalt und Umfang des Schutzes von Geschäftsgeheimnissen nach der Richtlinie (EU) 2016/943 (Richtlinie (EU) 2016/943), WRP 2017, 1034 (1038).

[52] Ausführlicher *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (292).

[53] Ausführlicher *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (292 f mwN).

[54] Ibid.

zugänglich ist.[55] Dabei ist auf den Personenkreis abzustellen, der üblicherweise mit Informationen der jeweiligen Art umgeht. Angesichts dessen herrscht Einigkeit, dass die Informationen nicht „absolut", sondern nur „relativ" geheim sein müssen.[56]

Prima facie ist die Bestimmung dieses geheimen Charakters in Big Data-Sachverhalten besonders schwierig, denn die in diesem Rahmen genutzten Datensets zeichnen sich typischerweise durch eine besondere Vielfalt (Variety) aus.[57] 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 noch ohne Weiteres zugänglich.[58] 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.[59] 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 im Sinne der Richtlinie auf.[60] Gleiches gilt für neue Erkenntnisse, die aus dem Datenset abgeleitet werden, wie beispielsweise das (prognostizierte) Kaufverhalten bestimmter Kundengruppen. Ebenso weisen Datensammlungen, wie sie etwa im Kontext von *Text-* und *Data-Mining* oder im Zusammenhang mit dem Training *Künstlicher Intelligenz* (maschinelles Lernen) aggregiert, normalisiert und strukturiert werden (sog. *Korpora*[61]), regelmäßig einen geheimen Charakter auf. Dies gilt entsprechend für neuronale Netze, die im Rahmen maschinellen Lernens entstehen.[62]

Da Art. 2 Nr. 1 lit. a TS-RL 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 regelmäßig einen geheimen Charakter aufweisen.[63]

---

55 Zu frei verfügbaren Datensets bspw im Rahmen der Open-Data-Bewegung vgl *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (293 mwN).
56 Vgl *Sousa e Silva*, What exactly is a trade secret under the proposed directive?, JIPLP 2014, 923 (928 f mwN).
57 Vgl bereits *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (293 mwN).
58 Ebenso *Drexl*/*Hilty*/*Desaunettes et al*, GRUR Int 2016, 914 (916 f).
59 Ausführlicher *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (294).
60 Vgl dazu *Drexl*/*Hilty*/*Desaunettes et al*, GRUR Int 2016, 914 (916 f).
61 Vgl zu Begriff und Bedeutung der *Korpora* oben B. I. 1. b).
62 Ebenso *Surblyte*, Data-Driven Economy and Artificial Intelligence: Emerging Competition Law Issues?, WUW 2017, 120 (125).
63 *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (295).

Datensets (strukturiert und unstrukturiert) sind vor diesem Hintergrund für sich betrachtet regelmäßig geheim im Sinne des Art. 2 Nr. 1 lit. a TS-RL. 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.[64] 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.[65] Gleiches gilt für den (partiellen) Austausch im Rahmen kooperativer Netzwerke. Unklar bleibt allerdings, wie vielen Personen Zugriff auf ein Datenset eingeräumt werden darf, ohne dass dessen geheimer Charakter verloren geht.[66] Aus dem Sinn und Zweck der Richtlinie – Innovationsförderung durch Geheimnisschutz[67] – lässt sich allerdings ableiten, dass der relativ geheime Charakter fortbesteht, wenn und soweit die Ausweitung des Kreises (potenzieller) Mitwisser durch den konkreten Zweck der jeweiligen Unternehmung gerechtfertigt ist.[68] 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.

Zudem könnte der geheime Charakter bei personenbezogenen Datensets entfallen, wenn und weil die betreffenden Personen ihre Auskunftsrechte etwa nach Art. 15 DSGVO geltend machen (können). Allerdings bleiben die genaue Anordnung und Zusammensetzung der Datensets trotz Bestehen bzw. Geltendmachung eines Auskunftsrechts geheim. Denn zum einen ist der Kreis der auskunftspflichtigen Informationen eng begrenzt[69]; zum anderen haben die betroffenen Personen stets nur ein Recht auf Auskunft über ihre personenbezogenen Daten.[70]

---

64 Vgl *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (295 f).

65 Ibid.

66 Ibid.

67 Vgl Erwägungsgründe 1-4, 8 TS-RL; allgemein zur umstrittenen theoretischen Rechtfertigung des Geheimnisschutzes *Ohly*, Der Geheimnisschutz im deutschen Recht: heutiger Stand und Perspektiven, GRUR 2014, 1 (2 f mwN); *Lemley*, The surprising virtues of treating trade secrets as IP rights, 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* Enhancing TRIPS: Trade Secrets and Reverse Engineering in Ullrich/Hilty/Lamping et al (Hg) TRIPS plus 20 (Berlin/Heidelberg 2016) 725 (734 f mwN).

68 *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (296).

69 Vgl *Rühlicke*, Die Geheimhaltung von Scoring-Algorithmen in Maute/Mackenrodt (Hg) Recht als Infrastruktur für Innovation (Baden-Baden 2019) 9 (24 ff).

70 Vgl allerdings zur Möglichkeit der Bündelung von Anfragen sowie des *Reverse Engineerings Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (306 f) sowie am Beispiel des Projekts „Open-Schufa – Wir knacken die Schufa" *Rühlicke*, Die Geheimhaltung von Scoring-Algorithmen (Fn 69) 9 (12). Zur Auswertung der an OpenSchufa „gespendeten" Datensätze vgl nun http://web.br.de/interaktiv/erhoehtes-risiko/; http://www.spiegel.de/wirtschaft/service/schufa-so-funktioniert-deutschlands-einflussreichste-auskunftei-a-1239214.html. Speziell zum Schutz von Geschäftsgeheimnissen vor dem datenschutzrechtlichen Auskunftsanspruch nach Art 15 DSGVO vgl *Ziegelmayer*, Geheimnisschutz ist eine große Niesche, CR 2018, 693 (697) mwN.

dd) Zwischenergebnis

Als Zwischenergebnis bleibt somit festzuhalten: Datensets (strukturiert und unstrukturiert) sind regelmäßig von potenziell kommerziellem Wert und geheim. Gleiches gilt für neue Informationen, die aus den Datensets abgeleitet wurden (derivative Daten). Der Schutz erstreckt sich zugleich auf die Metadaten, die regelmäßig in ihrer genauen Anordnung und Zusammensetzung ebenfalls geheim sind. Zudem weisen sie in der Regel einen kommerziellen Wert auf, weil sich mit ihrer Hilfe Datensets so strukturieren und veredeln lassen, dass aus ihnen neue Erkenntnisse abgeleitet werden können.

c) Algorithmen, neuronale Netze und Software-Implementierungen

Algorithmen[71] 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.[72] Deshalb sind Algorithmen dem Wortlaut des Art. 2 Nr. 1 TS-RL nach grundsätzlich als Geschäftsgeheimnisse zu qualifizieren. Dieser weitgehende Schutz von Algorithmen erstaunt,[73] widerspricht er doch der gesetzgeberischen Grundentscheidung, abstrakte Methoden, Ideen und Lehren gemeinfrei zu halten.[74] 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*.[75] Dies setzt einen Anreiz, Algorithmen unter angemessenen Bedingungen offenzulegen. Somit steht der Geheimnisschutz von Algorithmen in vollem Einklang mit dem Sinn und Zweck der Richtlinie. Allerdings sind Algorithmen aus dem Schutzbereich des Geheimnisschutzes auszuklammern, wenn und soweit sie in den maßgeblichen Kreisen im Sinne von Art. 2 Nr. 1 lit. a TS-RL „allgemein

---

71 Zur Definition des Begriffs Algorithmus vgl Fn 22.

72 *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (296 f). Zurückhaltender *Surblyte*, WUW 2017, 120 (126); *Mattioli*, Minn L Rev 2014, 535 (552 f) (aus Sicht des *Trade-Secrets*-Rechts der USA).

73 Zur weiten Schutzwirkung des Geheimnisschutzes nach der neuen Richtlinie B. III. 1.

74 *De lege lata* existiert daher kein sonderrechtlicher Schutz für Algorithmen. Im Rahmen der RL 2009/24/EG über den Rechtsschutz von Computerprogrammen v 23.4.2009, ABl 2009 L 111, 16 (Computerprogramm-Richtlinie) werden allgemeine Algorithmen gezielt ausgeklammert, vgl dazu ausführlicher *Triebe*, Reverse Engineering im Lichte des Urheber- und Geschäftsgeheimnisschutzes, 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 (München 2015), 29 ff mwN. Zusammenfassend *Scheja*, CR 2018, 485 (486 f mwN).

75 Zum *Reverse-Engineering* von Algorithmen vgl Fn 70; speziell zu Deep-Learning-Algorithmen *Goldfarb/Gans/Agrawal*, Prediction Machines: The Simple Economics of Artificial Intelligence, (Boston, Massachusetts 2018), 202 ff mwN.

bekannt“ oder „ohne Weiteres zugänglich“[76] sind oder als „belanglose Information“ im Sinne des Erwägungsgrundes 14 S. 5 TS-RL zu qualifizieren sind. Über diese begrenzenden Kriterien kann zumindest elementaren Freihaltebedürfnissen Rechnung getragen werden. Überdies folgt aus Art. 3 Abs. 1 lit. a TS-RL, dass unabhängig entdeckte bzw. entwickelte Algorithmen frei verwendet werden können. Computerprogramme, die entsprechende Algorithmen implementieren, genießen ebenfalls im Grundsatz Geheimnisschutz.[77] Gleiches gilt für neuronale Netze und separat gespeicherte Gewichtungsmatrizen.[78]

d) Übergreifendes Kriterium: Angemessene Geheimhaltungsmaßnahmen im Sinne des Art. 2 Nr. 1 lit. c TS-RL

Datensets (strukturiert und unstrukturiert, samt Metadaten), neuronale Netze, Algorithmen und entsprechende Software-Implementierungen erfüllen somit in der Regel die Kriterien des kommerziellen Werts und des geheimen Charakters. Darüber hinaus muss der potenzielle Geheimnisinhaber den Umständen entsprechende, angemessene Geheimhaltungsmaßnahmen im Sinne des Art. 2 Nr. 1 lit. c TS-RL treffen.[79] Bei Sachverhalten im Kontext der Datenwirtschaft werden regelmäßig angemessene Geheimhaltungsmaßnahmen im Sinne des Art. 2 Nr. 1 lit. c TS-RL vorliegen. Denn datenverarbeitende Stellen müssen aus Gründen des Datenschutzes und der IT-Sicherheit ohnehin weitreichende technisch-organisatorische Schutzmaßnahmen ergreifen [80] Richtigerweise sind zudem keine strengen Anforderungen an die Angemessenheit der Maßnahmen zu stellen. Es genügt, wenn der Geheimnisinhaber das jeweilige Minimum an Schutzvorkehrungen getroffen hat, das erforderlich ist, um die spezielle Information innerhalb des betreffenden

---

[76] Vgl *Scheja*, CR 2018, 485 (490), die im Rahmen der allgemeinen Zugänglichkeit darauf abstellt, ob der Algorithmus ohne weiteres „herstellbar“ ist.

[77] Ausführlicher *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (297-298 mwN).

[78] Ausführlicher *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (294-295 mwN); *Ehinger*/*Stiemerling*, CR 2018, 761 (762 ff.) mit dem 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.

[79] Ausführlich hierzu *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (298-302 mwN); *Scheja*, CR 2018, 485 (490).

[80] Vgl *Scheja*, CR 2018, 485 (490-492); *Heinzke*, Richtlinie zum Schutz von Geschäftsgeheimnissen, CCZ 2016, 179 (182); *Müllmann*, Auswirkungen der Industrie 4.0 auf den Schutz von Betriebs- und Geschäftsgeheimnissen, WRP 2018, 1177 (1182). Zu den erforderlichen Maßnahmen zum Schutz personenbezogener Daten, vgl insb Art 32 Abs 1 DSGVO; dazu *Martini* in BeckOK Datenschutzrecht DSGVO (2018) Art 24 Rn 20 ff, Art 32 Rn 1 ff. Zu den einzuhaltenden IT-Sicherheitsstandards, vgl insb §§ 8a, 8c BSIG; s dazu *Frisse*/*Glaßl*/*Baranowski et al*, Unternehmenssicherheit bei Banken – IT-Sicherheit, Know-how Schutz, Datensicherheit und Datenschutz, BKR 2018, 177 (179 ff mwN) sowie speziell zur Richtlinie 2016/1148/EU über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union v 06.07.2016, ABl 2016 L 194, 1 (NIS-Richtlinie) https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html. Speziell zu den Anforderungen an Cloud-Kunden und Cloud-Anbieter aus DSGVO und NIS-Richtlinie *Hofmann*, ZD-Aktuell 2017, 06488 mwN. Insbesondere im Hinblick auf das nach der TS-RL zulässige *Reverse Engineering* sind darüber hinaus vertragliche Regelungen ratsam, vgl dazu Fn 70.

Personenkreises geheim zu halten.[81] Im Rahmen typischer Big Data-Sachverhalte wird das Kriterium der angemessenen Geheimhaltungsmaßnahmen im Sinne des Art. 2 Nr. 1 lit. c TS-RL somit regelmäßig erfüllt sein.

e) Zwischenergebnis

Zusammenfassend lässt sich festhalten: Datensets (strukturiert und unstrukturiert, samt Metadaten), neuronale Netze, Algorithmen und entsprechende Software-Implementierungen genießen in der Regel Geheimnisschutz.

3. Datenbankschutz in typischen Big Data-Sachverhalten

a) Allgemeiner Geltungsbereich der DB-RL: Datenbank im Sinne des Art. 1 DB-RL

Die Datenbank-Richtlinie eröffnet ihren Anwendungsbereich ebenso wie die Trade-Secrets-Richtlinie mit einer weiten, technologieneutralen Definition, Art. 1 DB-RL.[82] Umfasst sind Datenbanken in jeglicher Form, d.h. Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind, Art. 1 Abs. 1, 2 DB-RL.[83]

Zwar sind damit Einzeldaten[84] und gänzlich unstrukturierte Datensets („Datenhaufen") vom unmittelbaren Schutzbereich der Datenbank-Richtlinie ausgenommen.[85] Vor dem Hintergrund der weiten Definition besteht allerdings weitgehend Einigkeit, dass die Mehrheit der Big Data-Datensets als Datenbanken im Sinne von Art. 1 DB-RL zu qualifizieren sind.[86] Insbesondere erfüllen Datensets, die im Kontext von *Text-* und *Data-Mining*[87] oder im Zusammenhang mit dem Training *Künstlicher Intelligenz* aggregiert, normalisiert und strukturiert werden (sog. *Korpora*[88]), regelmäßig die

---

81 *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (299-301); aA *Alexander*, WRP 2017, 1034 (1039), der ohne Begründung davon ausgeht, dass ein Minimum an Schutzvorkehrungen nicht genügt.

82 Der EuGH betont in einer Reihe von Urteilen, dass der Datenbankbegriff weit auszulegen sei, vgl EuGH GRUR 2005, 254 Rn 23 ff – Fixtures Marketing Ltd/Organismos prognostikon agonon posdosfairou AE; EuGH GRUR 2015, 253 Rn 33 – Ryanair/PR Aviation. Eine zusätzliche Ausweitung erfährt die Datenbank-Definition dadurch, dass der EuGH das hauptlimitierende Kriterium – die Unabhängigkeit der Elemente – extensiv ausgelegt s EuGH GRUR 2015, 1187 Rn 21 ff, 28 f – Freistaat Bayern/Verlag Esterbauer. Vgl dazu insgesamt *Wiebe*, GRUR 2017, 338 (339 mwN); *Hertin*, Der Elementenschutz für Darstellungen wissenschaftlicher und technischer Art ist eröffnet – Die Konsequenz aus der Rechtsprechung des EuGH zum Datenbankschutz für analoge Kartographie, in Dreier/Peifer/Specht (Hg) Anwalt des Urheberrechts (München 2017) 13 (19 ff mwN). Zu Vorschlägen *de lege ferenda* zur Ausgestaltung und Begrenzung der Datenbank-Definition *JIIP*, Study (Fn 13) Annex 1: Legal Analysis, 13. Ausführlich zur Vielfalt geschützter Datenbanken *JIIP*, Study (Fn 13) 4-7, 77.

83 Dazu ausführlicher *Leistner*, The protection of databases in Derclaye (Hg) Research handbook on the future of EU copyright (Cheltenham 2009) 427 (429); *Bygrave*, The data difficulty in database protection, EIPR 2013, 25 (26 ff); *Wiebe*, GRUR 2017, 338 (339-341 mwN).

84 *Duisberg,* „Datenhoheit und Recht des Datenbankherstellers" (Fn 2) 16 (24).

85 S dazu im Einzelnen *Zech*/*Schmidt*, Datenbankherstellerschutz für Rohdaten, CR 2017, 417 (419 f mwN), die den Begriff „Datenhaufen" zu Recht eng als „willkürliche und unstrukturierte Datenanhäufung" verstehen; *Wiebe*, GRUR 2017, 338 (340 mwN).

86 Vgl dazu *Leistner*, Big Data (Fn 9) 27 Fn 2 mwN; in diese Richtung nun auch SWD(2018) 147 endg, 13, 23.

87 Zu Begriff und Bedeutung des *Text-* und *Data-Minings* Fn 37.

88 Zu Begriff und Bedeutung der *Korpora* Fn 39.

Voraussetzungen der Datenbank-Definition.[89] Für strukturierte Datensets samt Metadaten ist der Geltungsbereich der Datenbank-Richtlinie somit eröffnet.

b) Spezielle Schutzvoraussetzung des sui generis-Rechts: Wesentliche Investition im Sinne des Art. 7 Abs. 1 DB-RL

Um in den Genuss des *sui generis*-Rechts zu gelangen, muss der potenzielle Datenbankhersteller eine wesentliche Investition in die Beschaffung, Überprüfung oder die Darstellung des Datenbankinhalts tätigen, Art. 7 Abs. 1 DB-RL.

aa) Wesentlichkeitskriterium als de-minimis-Schwelle

Das Wesentlichkeitskriterium wird überwiegend als *de-minimis*-Schwelle verstanden,[90] so dass die Wesentlichkeitsschwelle in Big Data-Konstellationen im Regelfall überschritten wird.

bb) Investitionen in das „Beschaffen" der Datenbankinhalte

Allerdings ist umstritten, ob in typischen Big Data-Sachverhalten Aufwendungen getätigt werden, die als Investition in das „Beschaffen" der Datenbankinhalte qualifiziert werden können.[91] Die Kommission verneint dies mit der überwiegenden Meinung in der Literatur.[92] Diese Meinung beruht auf der Grundsatzentscheidung des EuGH in Sachen *BHB*/*Hill*[93] und den drei parallelen Urteilen in Sachen *Fixtures Marketing*[94]. In diesen Fällen hatte der EuGH den unbestimmten Rechtsbegriff der „wesentlichen Investition" im Sinne des Art. 7 Abs. 1 DB-RL erstmals konkretisiert. Eine schutzbegründende Investition tätigt danach nur, wer in die Beschaffung, d.h. in das „Ermitteln" existierender Elemente investiert. Irrelevant sind dagegen Investitionen in das „Erzeugen" neuer Elemente.

(1) Extensive Interpretation der Kommission und der überwiegenden Literatur

Die Kommission beruft sich mit der überwiegenden Literaturansicht auf diese Rechtsprechungsreihe und leitet daraus ab, dass die Investitionen in typischen Big Data-Konstellationen der letztgenannten

---

89 Vgl *Bitkom*, Stellungnahme im Rahmen der Konsultation der Europäischen Kommission zur Bewertung der Datenbankrichtlinie (Berlin 2017) 4, abrufbar unter https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Stellungnahme-zur-Konsultation-der-Europaeischen-Kommission-zur-Bewertung-der-Datenbankrichtlinie.html. Im Kontext des maschinellen Lernens sind die *Korpora* allerdings von neuronalen Netzen abzugrenzen, die beim Training *Künstlicher Intelligenz* auf Grundlage der *Korpora* entstehen: *Neuronale Netze* sind bereits nicht als Datenbank iSd Art 1 DB-RL zu qualifizieren, vgl im Einzelnen *Grützmacher*, Urheber-, Leistungs- und Sui-generis-Schutz von Datenbanken (Baden-Baden 1999) 172; *Ehinger*/*Stiemerling*, CR 2018, 761 (768-769 mwN).

90 Ausführlicher hierzu *Leistner*, Big Data (Fn 9) 27 (29 f mwN), der zu Recht darauf hinweist, dass eine derart extensive Auslegung der Wesentlichkeitsschwelle geboten ist, um Rechtssicherheit und effektive Harmonisierung zu gewährleisten; aA *Auer-Reinsdorff*, Schutz von Datenbanken und Datenbankwerken, in Conrad/Grützmacher (Hg) Recht der Daten und Datenbanken im Unternehmen (Köln 2014) 205 (216 mwN). Für einen Überblick über die mitgliedstaatliche Rechtsprechung vgl SWD(2018) 147 endg, 27-28 mwN; *JIIP*, Study (Fn 13) 7-9, 78 f mwN.

91 Vgl dazu *Leistner,* Big Data (Fn 9) 27-29 mwN.

92 Vgl Fn 14.

93 EuGH GRUR 2005, 244 (Rn 31-42) – The British Horseracing Board Ltd/William Hill Organization Ltd [BHB/Hill].

94 EuGH GRUR 2005, 254 (Rn 40-53) – Fixtures Marketing Ltd/Organismos prognostikon agonon posdosfairou AE; EuGH GRUR Int 2005, 244 (Rn 34-49) – Fixtures Marketing Ltd/Oy Veikkaus AB; EuGH GRUR 2005, 252 (Rn 24-37) – Fixtures Marketing Ltd/Svenska Spel AB.

Kategorie zugeordnet werden müssen: Aufwendungen für Sensoren oder Maschinen, die Daten messen, seien als irrelevante Investitionen in das „Erzeugen" neuer Elemente zu qualifizieren.

(2) Gebotene teleologische Interpretation der Abgrenzungskriterien „Ermitteln" vs. „Erzeugen" (teleologischer BHB/Hill-Test)

Die Trennlinie zwischen berücksichtigungsfähigen Investitionen in das „Beschaffen" und irrelevanten Aufwendungen für das „Erzeugen" der Datenbankinhalte ist in den Randbereichen in der Tat unscharf.[95] Dieser Befund rechtfertigt jedoch nicht die pauschale Aussage, dass das *sui generis*-Recht „im Großen und Ganzen nicht für die Datenwirtschaft" gelte.[96] Vielmehr müssen die Abgrenzungskriterien des EuGH differenziert nach ihrem Sinn und Zweck interpretiert und im Einzelfall angewandt werden.[97]

Der EuGH zielte mit der Einführung dieser Abgrenzungskriterien darauf ab, wettbewerbsfunktional problematische *Sole-Source*-Konstellationen[98] vom Schutzbereich des *sui generis*-Rechts auszuklammern. Vor diesem Hintergrund sollte man den Begriff des „Erzeugens" in einem engen Sinne als „Erfinden" neuer Daten verstehen.[99] Investitionen sind folglich nur dann vom Schutzbereich des *sui generis*-Rechts auszunehmen, wenn und soweit sie sich auf das „Erfinden" neuer Daten beschränken. Nur hier entsteht ein genuines Monopolisierungsproblem, weil die der Datenbank zugrunde liegenden Informationen nicht frei verfügbar sind und daher von einem konkurrierenden Drittanbieter aufgrund eigener Bemühungen nicht zusammengestellt und systematisiert werden können.

Anders gelagert sind Konstellationen, in denen Daten durch Feststellung in der Natur, Technik oder sonstigen Gebieten vorhandener Faktizitäten beschafft werden können. In derartigen Fällen kann sich ein potenzieller Konkurrent grundsätzlich mit identischem wirtschaftlichem Aufwand die fraglichen Daten selbst beschaffen. In solchen Konstellationen sind entsprechende Aufwendungen folglich als berücksichtigungsfähige Investitionen in das „Beschaffen" von Daten zu qualifizieren.[100] Es geht mit anderen Worten primär um eine Abgrenzung des „Erfindens" vom „Vorfinden" von Daten.[101] Diese teleologische Lesart der Abgrenzung hat sich auch in der – teils höchstrichterlichen – Rechtsprechung

---

95 Konkret zur Datenwirtschaft *Sattler*, Allgemeiner rechtlicher Rahmen in Sassenberg/Faber (Hg) Rechtshandbuch Industrie 4.0 (München 2017) 27 (35); allgemein: *Ehmann*, Big Data auf unsicherer Grundlage – was ist „wesentlich" beim Investitionsschutz für Datenbanken?, K&R 2014, 394 (397); *Leistner*, "Last exit" withdrawal?, K&R 2007, 457 (460 ff) je mwN.

96 So aber SWD(2018) 146 endg, 2; ausführlicher SWD(2018) 147 endg, 35-37, 47 mwN.

97 In diese Richtung bereits *Leistner*, Big Data (Fn 9) 27 (28 f mwN).

98 Dh Konstellationen, in denen die Daten nur aus einer Quelle verfügbar sind – insbesondere, wenn und weil sie vom Datenbankhersteller selbst erzeugt („erfunden") wurden, Bspe: Fernsehprogramme, Zugfahrpläne oder Zuordnung von Telefonnummern an Teilnehmer, vgl *Leistner*, K&R 2007, 457 (458).

99 Richtigerweise ist also zwischen einem unbeachtlichen Erzeugen im engeren Sinn („Erfinden" von neuen Elementen) und einem berücksichtigungsfähigen Erzeugen im weiteren Sinn („Vorfinden" bereits vorhandener Elemente) zu unterscheiden, vgl dazu *Leistner*, Big Data (Fn 9) 27 (28 f).

100 S *Leistner*, Datenbankschutz – Abgrenzung zwischen Datensammlung und Datengenerierung, CR 2018, 17 (20 f mwN); ähnlich auch *Ehmann*, K&R 2014, 394 (397); aA *Bygrave*, EIPR 2013, 25 (31).

101 *Leistner*, K&R 2007, 457 (460).

zahlreicher Mitgliedstaaten durchgesetzt (teleologischer *BHB*/*Hill*-Test).[102] In unterschiedlichen Sachverhaltskonstellationen haben namentlich BGH[103], österreichischer OGH[104] und der Court of Appeal of England and Wales[105] entschieden, dass Investitionen in die Einrichtung von Systemen berücksichtigungsfähig sind, wenn und soweit sie dazu dienen, geographische Daten, Spieldaten (Punktestand, Fouls, etc.), Umsatz- oder Nutzungsdaten zu ermitteln, zu messen oder zu dokumentieren.[106]

(3) Grenzfälle

Allerdings gibt es mehrere Grenzfälle, in denen es schwerfällt, eine genaue Trennlinie zwischen dem „Erzeugen" und dem „Ermitteln" von Daten zu ziehen.[107] Aus Platzgründen kann im Rahmen des Beitrags nur auf eine Kategorie von Grenzfällen eingegangen werden: Metadaten. Im Rahmen einer systematischen oder methodischen Strukturierung entstehen – wie oben dargelegt – notwendigerweise Metadaten. Insoweit erforderliche Aufwendungen sind auf den ersten Blick als irrelevante Investitionen in das „Erzeugen" neuer Daten zu qualifizieren. Allerdings ist die „Schaffung" von Metadaten nicht Bezugspunkt der Investitionen. Vielmehr beziehen sich entsprechende Investitionen auf die systematisch-methodische Strukturierung oder Verifikation bereits vorhandener Datenbankelemente. Es handelt sich insoweit folglich um berücksichtigungsfähige Investitionen in die „Darstellung" oder „Überprüfung" der Elemente.[108] Im Übrigen herrscht bis zu einer Konkretisierung durch den EuGH oder den Gesetzgeber erhebliche

[102] *Leistner,* Big Data (Fn 9) 27 (28 f); Begriff „teleologischer *BHB*/*Hill*-Test" nach *Leistner*, K&R 2007, 457 (460).

[103] BGH GRUR 2005, 858 – HIT BILANZ; vgl auch BGH GRUR 2010, 1005 – Autobahnmaut.

[104] OGH Urt v 24.3.2015 – 4 Ob 206/14v, BeckRS 2015, 81041: Anders als bei Datenbanken, die lediglich Pläne für künftige Ereignisse enthalten (vgl BHB/Hill [Pläne für Pferderennen] und die Fixtures-Marketing-Fälle [Fußballspielpläne]), liege eine wesentliche Investition vor, wenn in eine Datenbank (auch) Ergebnisse von Fußballspielen aufgenommen werden. Das Erfassen der Ergebnisse ist in diesem Fall Teil der Datensammlung und -aufbereitung, nicht Teil der Datenerzeugung, vgl dazu *Büchele*, Anmerkung öOGH, Urt v 24.3.2015 – 4 Ob 206/14v, Fußballdatenbank, SpuRt 2015, 162 (164 f).

[105] Court of Appeal of England and Wales [2013] EWCA Civ 27 – Dataco & Others/Stan James Plc & Others and Sportradar GmbH & Others, abrufbar unter http://www.bailii.org/ew/cases/EWCA/Civ/2013/27.html: „facts observed – such as the scoring of a goal in football – are not ‚created data'", vgl dazu *Hugenholtz*, Something Completely Different: Europe's Sui Generis Database Right, in Frankel/Gervais (Hg) The internet and the emerging importance of new forms of intellectual property (Alphen aan den Rijn 2016) 205 (213).

[106] Die Kommission bezeichnet die Frage, ob das Aufzeichnen bestehender Daten als „Beschaffen" iSd Art 7 Abs 1 DB-RL zu qualifizieren ist, zwar als zentrale Frage („key question"), vgl SWD(2018), 147 endg, 25. Zum einen wird die mitgliedstaatliche Rechtsprechung aber nicht vollständig ausgewertet. Zum anderen fehlt es an einer begründeten Stellungnahme. Eine solche wäre dringend erforderlich gewesen, da die Auffassung der Kommission der höchstrichterlichen Rechtsprechung in zahlreichen Mitgliedstaaten – wie gezeigt – diametral entgegensteht.

[107] Zur Echtzeiterfassung von Maschinendaten vgl *Sattler*, Allgemeiner rechtlicher Rahmen (Fn 95) 27 (35); SWD(2018) 146 endg, 15. Zu Investitionen, die iRv Blockchain-Anwendungen getätigt werden vgl *Willecke*, Die urheberrechtliche Schutzfähigkeit von Blockchain-Anwendungen in Taeger (Hg) Recht 4.0 – Innovationen aus den rechtswissenschaftlichen Laboren (Edewecht 2017) 833 (839).

[108] Vgl dazu ausführlicher *Leistner*, CR 2018, 17 (19 f), der Aufwendungen für die Erstellung der Metadaten als Investitionen in die „Darstellung" qualifiziert. Zu den Definitionen der „Darstellung" und der „Überprüfung" iSd Art 7 Abs 1 DB-RL Fn 112 und 113.

Rechtsunsicherheit, inwieweit Investitionen in typischen Big Data-Konstellationen als schutzbegründendes „Beschaffen" oder als irrelevantes „Erzeugen" zu qualifizieren sind.[109]

(4) Zwischenergebnis: Investitionen in das „Beschaffen" von Datenbankinhalten in typischen Big Data-Konstellationen

Investitionen in die Entwicklung und Konfiguration von Mess- bzw. Abfragesystemen wirken nach richtiger Ansicht regelmäßig schutzbegründend. In einer Vielzahl von Big Data-Konstellationen genießen maschinengenerierte Daten daher mittelbaren Schutz durch das Datenbankherstellerrecht.[110] Gleiches gilt für personenbezogene Daten, wenn und soweit wesentliche Aufwendungen für die Entwicklung und Konfiguration entsprechender Mess- bzw. Abfragesysteme getätigt wurden.

cc) Weitere Anknüpfungspunkte für berücksichtigungsfähige Investitionen in typischen Big Data-Sachverhalten

In typischen Big Data-Sachverhalten werden zudem weitere Aufwendungen getätigt, die als schutzbegründende Investitionen qualifiziert werden können. So ist in der Regel eine kostenintensive Verifizierung, systematische oder methodische Strukturierung und ggf. Aktualisierung der Datenbankinhalte erforderlich.[111] Hierauf gerichtete Aufwendungen lassen sich als berücksichtigungsfähige Investitionen in die „Überprüfung"[112] bzw. „Darstellung"[113] der Datenbankinhalte im Sinne des Art. 7 Abs. 1 DB-RL qualifizieren, wenn sie sich von einer etwaigen „Erzeugung" der Rohdaten abgrenzen lassen.[114] Hierzu zählen namentlich die erforderlichen Aufwendungen für Anschaffung, Anmietung, Administration und Aktualisierung moderner IT-Infrastruktur (Webserver, sonstige Hardware, Cloud-Lösungen) samt Datenbank-Management- und Analysesoftware.[115]

---

[109] Relative Rechtssicherheit lässt sich allerdings durch alternative Gestaltungsmodelle erzielen, vgl hierzu *Sattler*, Allgemeiner rechtlicher Rahmen (Fn 95) 27 (35).

[110] *Leistner*, Big Data (Fn 9) 27 (29, 54 f).

[111] Vgl B. I. 1. a), b).

[112] Erfasst die Mittel, die „der Kontrolle der Richtigkeit der ermittelten Elemente bei der Erstellung der Datenbank und während des Zeitraums des Betriebes dieser Datenbank gewidmet werden […], um die Verlässlichkeit der in der Datenbank enthaltenen Investitionen sicherzustellen.", vgl EuGH GRUR 2005, 252 (Rn 27) – Fixtures Marketing Ltd/Svenska Spel AB; dazu im Einzelnen *Derclaye*, The Legal Protection of Databases (Cheltenham 2008) 97 mwN.

[113] Erfasst die Mittel, „mit denen [der] Datenbank ihre Funktion der Informationsverarbeitung verliehen werden soll, dh die Mittel, die der systematischen oder methodischen Anordnung der in der Datenbank enthaltenen Elemente und der Organisation der individuellen Zugänglichkeit dieser Elemente gewidmet werden.", vgl EuGH GRUR 2005, 252 (Rn 27) – Fixtures Marketing Ltd/Svenska Spel AB; dazu im Einzelnen *Derclaye*, The Legal Protection of Databases (Fn 112) 97-99.

[114] *In praxi* ist daher eine genaue Dokumentation der Kosten, die für die „Überprüfung" bzw „Darstellung" der Datenbankinhalte aufgewandt wurden, ratsam. Die Kommission erkennt diese zusätzlichen Anknüpfungspunkte im Rahmen der zweiten Evaluation im Grundsatz, bleibt allerdings bei den Schlussfolgerungen denkbar vage: „This might influence the legal regulation of the emerging data-driven business models building on 'big data' analytics of machine-generated, Internet of Things data.", vgl SWD(2018), 147 endg, 25.

[115] Vgl allgemeiner (erforderliche Soft- und Hardware) *Götz*, Big Data und der Schutz von Datenbanken, in Taeger (Hg) Big Data & Co, (Edewecht 2014) 19 (28 mwN); vgl auch *Derclaye*, The Legal Protection of Databases (Fn 112) 95.

dd) Ausschluss typischer Big Data-Datenbanken nach der Spin-off-Theorie?

Zusätzliche Rechtsunsicherheit herrscht überdies in allen Konstellationen, in denen Datenbanken als reines Nebenprodukt („*spin off*“) einer anders ausgerichteten geschäftlichen Haupttätigkeit entstehen – also in einer Vielzahl von Sachverhalten im Kontext der Datenwirtschaft. Nach der sog. *Spin-off*-Theorie sollen derartige Datenbanken vom Schutzbereich des *sui generis*-Rechts ausgeklammert werden.[116] Bis heute ist umstritten, ob der EuGH dieser Theorie folgt.[117] Der eben skizzierte Schutzbereich des Datenbankherstellerrechts würde dadurch jedenfalls erheblich reduziert.

Richtigerweise ist davon auszugehen, dass der EuGH die *Spin-off*-Theorie in seinen vier Grundsatzentscheidungen verworfen hat.[118] Wenn die Befürworter der *Spin-off*-Theorie – denen sich in jüngster Zeit auch die Kommission[119] angeschlossen hat – die Äußerungen des EuGH enger verstehen, tragen sie für diese Lesart die Begründungslast. Denn im Richtlinientext finden sich keine Anhaltspunkte für eine derartige Beschränkung des Schutzgegenstands. Zudem würde die *Spin-off*-Theorie weitere Abgrenzungsschwierigkeiten und damit erhebliche Rechtsunsicherheit hervorrufen.[120]

ee) Zwischenergebnis

In typischen Big Data-Konstellationen genießen maschinengenerierte und personenbezogene Daten mittelbaren[121] Schutz durch das Datenbankherstellerrecht.

Zwar ist die Abgrenzung zwischen schutzbegründendem „Beschaffen“ und irrelevantem „Erzeugen“ von Datenbankinhalten bis zu einer Konkretisierung durch den EuGH oder den Gesetzgeber mit erheblicher Rechtsunsicherheit verbunden. In konsequenter Anwendung des

---

[116] Vgl zusammenfassend *Ehmann*, K&R 2014, 394 (397 mwN).

[117] Dagegen: *Aplin*, The ECJ elucidates the database right, IPQ 2005, 204 (212); *Derclaye*, The Legal Protection of Databases (Fn 112) 94 („implicitly”); *Leistner*, Anmerkung zu EuGH Urt v 9.1.2004 – Rs C-203/02, JZ 2005, 408 (409). Befürwortend: *Davison/Hugenholtz*, Football fixtures horseraces and spin offs – the ECJ domesticates the database right, EIPR 2005, 113 (114). Der *Spin-off*-Theorie zugeneigt *Ehmann*, K&R 2014, 394 (398 f).

[118] S EuGH GRUR 2005, 244 (Rn 35) – BHB/Hill; EuGH GRUR 2005, 254 (Rn 45) – Fixtures Marketing Ltd/Organismos prognostikon agonon posdosfairou AE; EuGH GRUR Int 2005, 244 (Rn 39) – Fixtures Marketing Ltd/Oy Veikkaus AB; EuGH GRUR 2005, 252 (Rn 29) – Fixtures Marketing Ltd/Svenska Spel AB: „In diesem Zusammenhang schließt der Umstand, dass die Erstellung einer Datenbank mit der Ausübung einer Haupttätigkeit verbunden ist, in deren Rahmen die Person, die die Datenbank erstellt, auch die in dieser Datenbank enthaltenen Elemente erzeugt, als solcher nicht aus, dass diese Person den Schutz durch das Schutzrecht *sui generis* beanspruchen kann, sofern sie nachweist, dass die Beschaffung dieser Elemente, ihre Überprüfung oder ihre Darstellung […] Anlass zu einer in quantitativer oder qualitativer Hinsicht wesentlichen Investition gegeben haben, die im Verhältnis zu den Mitteln selbständig ist, die eingesetzt worden sind, um diese Elemente zu erzeugen.“.

[119] S SWD(2018) 146 endg, 2; ausführlicher SWD(2018) 147 endg, 15, 24 f, 35-37; zurückhaltender *JIIP*, Study (Fn 13), Annex 1: Legal Analysis, 65.

[120] Vor diesem Hintergrund bereits gegen eine parallele Theorie im Rahmen des Geheimnisschutzes *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (302 mit Fn 80).

[121] Zum mittelbaren Schutz von Einzeldaten durch den Datenbankschutz *Duisberg,* „Datenhoheit und Recht des Datenbankherstellers“ (Fn 2) 16 (24).

teleologischen *BHB*/*Hill*-Tests sind die Aufwendungen in typischen Big Data-Sachverhalten aber als schutzbegründende Investitionen in das „Beschaffen" von Daten zu qualifizieren.[122]

Selbst wenn Aufwendungen im Einzelfall als irrelevantes „Erzeugen" qualifiziert werden sollten, bieten sich in Big Data-Sachverhalten mit der notwendigen „Überprüfung" und „Darstellung" der Datenbankinhalte stets zwei weitere Anknüpfungspunkte an. Voraussetzung ist allerdings, dass sich die entsprechenden Investitionen von irrelevanten Aufwendungen für ein etwaiges „Erzeugen" der Rohdaten abgrenzen lassen.[123]

4. Fazit

Zusammenfassend bleibt festzuhalten: Einzeldaten genießen für sich betrachtet weder Datenbank- noch Geheimnisschutz. Hierdurch entstehen aber keine ungewollten Schutzlücken. Vielmehr werden Einzeldaten aus guten Gründen aus dem Schutzbereich ausgeklammert: Sie sind weder schutzwürdig noch schutzbedürftig. An der Schutzwürdigkeit fehlt es, weil Informationen für sich betrachtet möglichst frei von exklusiven Zuordnungen bleiben sollten.[124] An der Schutzbedürftigkeit fehlt es, weil sie im Rahmen der Analyse notwendigerweise kontextualisiert und in Datensets überführt werden müssen. Als deren Bestandteil kommen sie mittelbar in angemessenem Umfang in den Genuss des Geheimnis- und/oder des Datenbankschutzes.

Zwar greift der Datenbankschutz erst, wenn wesentliche Investitionen in die Beschaffung, Überprüfung oder Darstellung der Einzel- bzw. Rohdaten geflossen sind. Im Rahmen typischer Big Data-Sachverhalte sind derartige Investitionen aber – wie gezeigt – kraft Natur der Sache erforderlich. Dabei werden nach richtiger Auffassung regelmäßig nicht nur schutzbegründende Investitionen in

---

[122] Aus Gründen der Rechtsklarheit sollte diese teleologische Interpretation im Gesetzestext verankert werden, vgl dazu den Vorschlag zur Neufassung des Art 7 Abs 1 DB-RL *Kur/Hilty/Geiger et al*, First Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Comment by the Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich, IIC 2006, 551 (556): „Die Mitgliedstaaten sehen für den Hersteller einer Datenbank, bei der für die Beschaffung, die Überprüfung oder die Darstellung ihres Inhalts eine in qualitativer oder quantitativer Hinsicht wesentliche Investition erforderlich ist, das Recht vor, die Entnahme und/oder die Weiterverwendung der Gesamtheit oder eines in qualitativer oder quantitativer Hinsicht wesentlichen Teils des Inhalts dieser Datenbank zu untersagen. Betrifft die wesentliche Investition das Erzeugen von Daten, die den Inhalt der Datenbank bilden, entsteht das sui generis-Recht insoweit nicht, als der Datenbankhersteller sich die betreffenden Daten ausgedacht hat oder diese erfunden hat, es sei denn, sie resultieren aus der Messung und/oder Sammlung bereits existenter Phänomene." (Übersetzung des Verf).

[123] Vgl zu den damit verbundenen Abgrenzungsschwierigkeiten im Kontext der Datenwirtschaft *Sattler,* Allgemeiner rechtlicher Rahmen (Fn 95) 27 (35 mwN), der dafür plädiert, Investitionen in die Datensystematisierung als Investition iSd Art 7 Abs 1 DB-RL anzusehen, ganz gleich, ob die jeweiligen Inhalte der Datenbank „beschafft" oder „erzeugt" wurden.

[124] Die zivilrechtliche Informationsordnung ist durch den Grundsatz des Gemeingebrauchs geprägt, vgl ausführlich *Wiebe*/*Schur*, ZUM 2017, 461 (464 ff) mit Verweis auf BVerfG NJW 1984, 419 (422) – Volkszählungsurteil: „Der einzelne [...] ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann." Zu Recht verweisen *Wiebe/Schur* darauf, dass Messdaten ebenfalls Abbild sozialer Realität sind. Vgl speziell zur TS-RL auch Erwägungsgrund 16 S 1 TS-RL. Zur Informationsfreiheit C.

die Überprüfung oder Darstellung der Daten fließen, sondern auch in die Beschaffung der Einzel- bzw. Rohdaten.

Überdies genießen Rohdaten regelmäßig unmittelbaren Geheimnisschutz. Für strukturierte Datensets mit geheimem Charakter verdoppelt die Trade-Secrets-Richtlinie sogar den Schutz: Unveröffentlichte Datenbanken genießen kumulativ Datenbank- und Geheimnisschutz.

Schließlich unterfallen Algorithmen und deren Software-Implementierungen regelmäßig dem Geheimnisschutzregime. Neuronale Netze sind zwar nicht als Datenbank zu qualifizieren; sie sind aber regelmäßig als Geschäftsgeheimnis geschützt.

Insgesamt genießen damit bereits *de lege lata* alle schutzwürdigen und schutzbedürftigen Bestandteile eines typischen Big Data-Prozesses Geheimnis- und/oder Datenbankschutz.

II. Schutzsubjekt

1. Ausgangspunkt: Vage Legaldefinition im Rahmen des Datenbank- und Geheimnisschutzes

Obwohl die Frage, wem das Datenbankherstellerrecht bzw. das Geschäftsgeheimnis zugeordnet wird, von zentraler Bedeutung ist, begnügen sich Datenbank- und Trade-Secrets-Richtlinie jeweils mit vagen Beschreibungen des Rechtsinhabers:

- Datenbankhersteller ist nach Erwägungsgrund 41 S. 2 DB-RL die Person, die die Initiative ergreift und das Investitionsrisiko trägt.[125]
- Geheimnisinhaber ist nach Art. 2 Nr. 2 TS-RL jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis besitzt.

Damit bleibt insbesondere offen, wem das Datenbankherstellerrecht bzw. das Geschäftsgeheimnis zuzuordnen ist, wenn mehrere Personen an der Entstehung der Datenbank bzw. des Geschäftsgeheimnisses beteiligt sind. Diese Unklarheit ist gerade im Kontext der Datenwirtschaft misslich, weil hier vernetzte Wertschöpfungsketten besonders häufig und im Interesse der Innovation besonders förderungswürdig sind.[126] Betrachtet man beispielsweise die Datenerhebung mittels Sensoren – etwa im Rahmen von Industrie 4.0 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?

[125] Dazu ausführlicher *Leistner,* Big Data (Fn 9) 27 (34 f mwN).
[126] Speziell zur TS-RL *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (303 f mwN). Allgemein zu diesem schutzrechtsübergreifenden Problem *Leistner*, Big Data (Fn 9) 27 (34-38, insb Fn 25).

- Oder ist es der konkrete Nutzer bzw. ein beteiligter Dienstleister?[127]

Die entsprechenden Fragen stellen sich für ein etwaiges Datenbankherstellerrecht: In der Regel lässt sich nicht klar bestimmen, wer die Initiative ergreift und das Investitionsrisiko trägt. Erschwerend kommt hinzu, dass die Regelungen in den mitgliedstaatlichen Umsetzungsakten erheblich divergieren.[128]

Werden die Datensets bzw. Algorithmen in einer vernetzten Umgebung gespeichert und ausgetauscht – wie es typischerweise im Kontext der Datenwirtschaft geschieht – erschwert dies die Zuordnung zusätzlich.[129] In vielen Fällen dürften dabei mehrere Beteiligte gemeinsam Inhaber eines Geschäftsgeheimnisses und/oder eines Datenbankherstellerrechts werden.[130]

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. Lösungsvorschläge zur rechtssicheren Konkretisierung des Rechtsinhabers: Privatautonome Regelungen und Registrierung im „Geheimnis- und/oder Datenbankschutzregister“

Relative Rechtssicherheit können die Beteiligten nur erzielen, indem sie vertragliche Vorkehrungen treffen.[131] Durch flexible privatautonome Gestaltung können etwaige Datenbankherstellerechte und Geschäftsgeheimnisse 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

---

[127] Vgl dazu das Roboter-Beispiel bei *Sattler*, Allgemeiner rechtlicher Rahmen (Fn 95) 27 (35).

[128] Vgl hierzu: SWD(2018) 147 endg, 26 f; *JIIP*, Study (Fn 13) 31, 78, sowie *JIIP*, Study (Fn 13) Annex 1: Legal Analysis, 45-51; *Koščík*/*Myška*, Database authorship and ownership of sui generis database rights in data-driven research, International Review of Law, Computers & Technology 2017, 43 (49-54, 58 mwN). Im Rahmen der Umsetzung der TS-RL drohen ähnliche Divergenzen zu entstehen, da die Definition des Geheimnisinhabers nur einen Mindeststandard vorgibt, vgl Art 1 Abs 1 UAbs 1 TS-RL.

[129] Zur verteilten Netzwerkstruktur im Rahmen typischer Big Data-Anwendungen vgl *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (303 f mwN). Zu den speziellen Zuordnungsproblemen in Industrie 4.0-Sachverhalten vgl *Müllmann*, WRP 2018, 1177 (1182).

[130] Zur DB-RL *Leistner*, Big Data (Fn 9) 27 (35). Zur TS-RL *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (303 ff mwN). Zu den daraus resultierenden Problemen allgemein *Drexl*/*Hilty*/*Globocnik et al*, Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission’s 'Public consultation on Building the European Data Economy', Max Planck Institute for Innovation & Competition Research Paper No 17-08 2017 1 (9). Die DB-RL überlässt die Ausgestaltung der gemeinsamen Inhaberschaft zudem komplett dem mitgliedstaatlichen Recht, wodurch die Rechtsunsicherheit in grenzüberschreitenden Konstellationen zusätzlich erhöht wird, vgl dazu *JIIP*, Study (Fn 13) Annex 1: Legal Analysis, 45 mwN. Mangels anderer Anhaltspunkte obliegt die Ausgestaltung der gemeinsamen Inhaberschaft im Rahmen der TS-RL ebenfalls dem mitgliedstaatlichen Recht.

[131] Zur DB-RL *Leistner*, Big Data (Fn 9) 27 (35-37 mwN); zur TS-RL *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (304 f mwN); ausführlich zur Ausgestaltung *in praxi* auch *Scheja*, CR 2018, 485 (488 f, 491 f mwN).

Konzept zur Ermittlung des „effektiven“ Geheimnisinhabers bzw. Datenbankherstellers zu entwickeln, dürften daher scheitern.[132]

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[133] und/oder die Schaffung vertragsrechtlicher Regelungen dispositiver und/oder zwingender Natur könnte allerdings dazu beitragen, diese Probleme zu reduzieren.[134]

Für den Bereich des Geheimnisschutzes könnte man flankierend ein Register mit fakultativer Eintragungsmöglichkeit etablieren.[135] Der Inhaber eines Geschäftsgeheimnisses könnte bei der Registrierung einen kryptographischen Fingerabdruck seiner geschützten Informationen hinterlegen.[136] Auf dieser Basis ließe sich die Inhaberschaft rechtssicher, geheimniswahrend und transaktionskostensparend dokumentieren, übertragen und lizenzieren.

Kooperationspartner und Arbeitnehmer könnten überdies ihre jeweiligen Arbeitsergebnisse im Geheimnisregister hinterlegen. Dadurch ließe sich im Streitfall klären, ob bzw. inwieweit Informationen von einem Kooperationspartner oder Arbeitnehmer geschaffen wurden. Dies erleichtert im ersten Schritt die Feststellung der originären Zuordnung. Im zweiten Schritt lässt sich

---

[132] Vgl allgemeiner zu den Problemen, die eine Zuordnung im Hinblick auf den Gleichheitssatz aufwirft, *Wiebe/Schur*, ZUM 2017, 461 (470, 473).

[133] Vgl zu Standardvertragsbedingungen für die gemeinsame Nutzung von Daten die „Contract Guidelines on Data Utilization Rights ver. 1.0 Formulated“ des Japanischen Ministry of Economy, Trade and Industry (METI), abrufbar unter http://www.meti.go.jp/english/press/2017/0530_002.html sowie die revidierte Fassung „Contract Guidance on Utilization of AI and Data“, abrufbar unter http://www.meti.go.jp/english/press/2018/0615_002.html. *Specht* verweist darauf, dass man sich bei der Entwicklung von Leitfäden und Standardvertragsklauseln partiell an den ausdifferenzierten Verträgen zur Nutzung von Geschäftsgeheimnissen orientieren könne, vgl *Specht*, Rechtsvergleichende Analyse (Fn 2) 9 (90).

[134] Vgl zur DB-RL *Leistner*, Big Data (Fn 9) 27 (38 f mwN); zur TS-RL *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (304 mwN). Vgl ferner den jüngst publizierten Leitfaden für die gemeinsame Nutzung von Daten des Privatsektors COM(2018) 232 endg, 1 f, 10 ff; SWD(2018) 125 endg, 6 ff.

[135] Die nach Art 17 TS-RL einzurichtenden Korrespondenzstellen könnten ein entsprechendes Register gemeinsam verwalten.

[136] Zur technischen Ausgestaltung *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (304-305 mit Fn 88); dort auch bereits zur möglichen Umsetzung eines solchen Registers auf Basis der Distributed-Ledger-Technologie Blockchain. Ausführlicher nun zur Distributed-Ledger-Technologie als Vehikel für die Zuordnung und Transaktion von Geschäftsgeheimnissen *Selz*, Zuordnung und Transaktion von Geschäftsgeheimnissen im Informationszeitalter in Taeger (Hg) Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht (Edewecht 2018) 411 (418 ff), der auf weitere Vorteile einer Registrierung von Geschäftsgeheimnissen hinweist. So ermöglicht der Registereintrag den Nachweis des rechtmäßigen Erwerbs eines Geschäftsgeheimnisses iSd Art 3 Abs 1 TS-RL, wenn und soweit der Hinterlegende anhand des Registereintrags nachweisen kann, dass er zu einem bestimmten Zeitpunkt bereits über eine konkrete Information verfügte. Insbesondere lässt sich auf diesem Weg ggf eine unabhängige Entdeckung oder Schöpfung iSd Art 3 Abs 1 lit a TS-RL nachweisen. Wenn die Registrierung des Geschäftsgeheimnisses vor der vermeintlichen Verletzungshandlung erfolgte, kann sich der mutmaßliche Verletzer jedenfalls gegen den Vorwurf eines unbefugten Zugangs iSd Art 4 Abs 2 lit a TS-RL verteidigen.

genau bestimmen, welche Informationen von etwaigen Rechteeinräumungen an die anderen Kooperationspartner oder den Arbeitgeber umfasst sind.[137]

Schließlich können die Parteien im Rahmen arbeitsvertraglicher Verschwiegenheitspflichten und sonstiger Geheimhaltungsvereinbarungen („*Non-Disclosure-Agreements*“, kurz: NDA) auf den kryptographischen Fingerabdruck verweisen. So lässt sich das zu schützende Geschäftsgeheimnis konkret identifizieren, ohne dass hierdurch das Risiko einer Offenlegung erhöht würde.

Im Bereich des Datenbankschutzes sprechen dagegen gute Gründe dafür, das Datenbankherstellerrecht in ein Registerrecht mit konstitutivem Eintragungserfordernis zu transformieren.[138] Das *sui generis*-Recht würde hierdurch funktional präziser an seinen Schutzzweck rückgebunden. Denn durch das Eintragungserfordernis wäre sichergestellt, dass nur derjenige ein *sui generis*-Recht erlangt, der dessen Schutz benötigt, um seine Investitionen zu amortisieren. Verlangt man überdies für jede Schutzfristverlängerung – gegebenenfalls progressiv ansteigende – Verlängerungsgebühren, ließe sich zugleich die Schutzdauer des *sui generis*-Rechts mit dessen Schutzzweck abstimmen. Insgesamt könnte ein konstitutives Eintragungserfordernis somit dazu beitragen, dass das Datenbankherstellerrecht im Einklang mit seinem Sinn und Zweck nur verliehen bzw. verlängert wird, wenn und soweit zusätzliche Anreize erforderlich sind, um eine Unterinvestition und damit Marktversagen auf den Datenmärkten zu verhindern. Es bedarf allerdings vertiefter Forschung, ob die Vorteile eines solchen konstitutiven Registrierungserfordernisses so stark sind, dass die damit verbundenen Risiken in Kauf genommen werden sollten.[139]

III. Schutzwirkung

1. Verstärkte „Verdinglichung“ des Geheimnisschutzes durch die Trade-Secrets-Richtlinie – flexible Freistellungen

Die neue Trade-Secrets-Richtlinie verstärkt die „Verdinglichung“ des Geheimnisschutzes: Der Inhaber eines Geschäftsgeheimnisses kann sich nun auf eine robuste Ausschlusswirkung gegenüber einem weit gefassten Kreis qualifizierter Dritter verlassen.[140]

---

[137] Der Bedarf nach einer solchen Lösung wird durch einen Blick in die Praxis bestätigt: Im Programmierbereich ist es bereits üblich, Datenbanken zu unterhalten, in denen die Entwickler die ihnen zugewiesenen Aufgaben, den Erledigungsstatus und ihre Arbeitsergebnisse hinterlegen, vgl zu dieser Praxis *Scheja*, CR 2018, 485 (489).

[138] Vgl dazu *Leistner*, Big Data (Fn 9), 27 (37 f mwN).

[139] Dazu ausführlicher ibid; in diese Richtung nun auch *JIIP*, Study (Fn 13) 64-71 mit der Darstellung verschiedener denkbarer Ansätze zur konkreten Ausgestaltung. Dort finden sich zudem die Stellungnahmen einiger Organisationen, die im Rahmen der zweiten Evaluation der DB-RL dafür plädierten, das *sui generis*-Recht in ein Registerrecht zu transformieren.

[140] Ausführlich *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (310 ff).

Im Interesse von Informationsfreiheit, Innovation und Wettbewerbsförderung sichert die Richtlinie andererseits wichtige Freiräume.[141] Die Verwendung einer Vielzahl unbestimmter Rechtsbegriffe und die einzelfallbezogene Verhältnismäßigkeitsprüfung auf Durchsetzungsebene eröffnen dabei gerade im Kontext der Datenwirtschaft einen breiten Spielraum für flexible Konkretisierungen.[142]

Zugleich resultiert daraus allerdings erhebliche Rechtsunsicherheit. Der genaue Umfang des Geheimnisschutzes im Bereich Big Data wird erst durch die mitgliedstaatlichen Gerichte bzw. den EuGH konturiert werden. Daher sollten die Generalklauseln und Freistellungen im Rahmen der Erwägungsgründe bzw. im Rahmen der nationalen Umsetzungsakte vor dem Hintergrund typischer Big Data-Konstellationen konkretisiert werden, um Rechtssicherheit und Rechtsklarheit zu schaffen.

2. Extensive Auslegung der Ausschließlichkeitsrechte im Rahmen des Datenbankschutzes – enge statische Ausnahmen

Die beiden Ausschließlichkeitsrechte des Art. 7 Abs. 2 DB-RL – „Entnahme“ und „Weiterverwendung“ – werden von der Rechtsprechung denkbar weit verstanden.[143]

Zwar bleibt die Entnahme bzw. Weiterverwendung unwesentlicher Teile einer Datenbank grundsätzlich erlaubt.[144] Big Data-Anwendungen erfordern allerdings die Aggregierung und Kombination *wesentlicher* Bestandteile verschiedener Datensets – idealerweise sogar *vollständiger* Datensets.[145] Denn erst auf dieser Basis können neue Erkenntnisse gewonnen werden. Die Begrenzung des Schutzgegenstandes auf wesentliche Teile einer Datenbank wird den Besonderheiten und Bedürfnissen der Datenwirtschaft somit nicht gerecht.[146]

---

[141] Ausführlich *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (306-309, 313 f). In Übereinstimmung mit dem Richtlinientext wurde § 5 des Referenten- bzw Regierungsentwurfes von einem Rechtfertigungsgrund zu einer Ausnahmebestimmung umgestaltet, vgl nun § 5 GeschGehG. Die Whistleblowing-Ausnahme, die auch im Kontext der Datenwirtschaft Bedeutung erlangen kann – man denke nur an die Aufdeckung mangelnder Daten- oder Algorithmenqualität –, wurde in der endgültigen Fassung modifiziert und objektiv formuliert, vgl nun § 5 Nr 3 GeschGehG.

[142] Zur besonderen Bedeutung eines flexiblen Rechtsrahmens für die dynamische datengetriebene Wirtschaft *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (315 f).

[143] Ausführlich hierzu *Leistner*, Big Data (Fn 9) 27 (30 f mwN); für einen Überblick über die Rechtsprechung des EuGH und der Mitgliedstaaten vgl SWD(2018) 147 endg, 28 f mwN sowie *JIIP*, Study (Fn 13) Annex 1: Legal Analysis, 66-69 mwN; speziell zu Metasuchmaschinen und *Screen-Scraping*-Fällen *Zech*/*Schmidt*, CR 2017, 417 (425 f).

[144] Ausführlich hierzu *Leistner*, Big Data (Fn 9) 27 (31 mwN). *Zech*/*Schmidt*, CR 2017, 417 (424, 426) bezeichnen die Freiheit der Nutzung unwesentlicher Teile der Datenbank bzw einzelner Daten als sekundären Zweck des *sui generis*-Rechts. Primärer Zweck des *sui generis*-Rechts ist der Investitionsanreiz durch Investitionsschutz.

[145] Ibid. Je größer die verfügbare Datenmenge ist, desto mehr Erkenntnisse lassen sich daraus ableiten, vgl *Kerber*, Rechte an Daten in der digitalen Ökonomie: Analyse öffentlicher Diskussionsprozesse und der in ihnen verwendeten Argumentation in ABIDA (Hg) Datenrechte – eine Rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA (Münster 2017) 115 (196 f mwN); zu den statistischen und ökonomischen Zusammenhängen vgl *Goldfarb/Gans/Agrawal*, Prediction Machines: The Simple Economics of Artificial Intelligence, (Boston, Massachusetts 2018), 49-51mwN.

[146] *Leistner*, Big Data (Fn 9) 27 (31 mwN); vgl dazu nun auch SWD(2018) 147 endg, 24.

Vor diesem Hintergrund ist es besonders misslich, dass die Ausnahmen des *sui generis*-Rechts[147] eng gefasst sind – sowohl im Vergleich zu den Freistellungen der Trade-Secrets-Richtlinie als auch im Vergleich zu den Schrankenkatalogen des allgemeinen Urheberrechts.[148] Angesichts der geschilderten Besonderheiten und Bedürfnisse der datengetriebenen Wirtschaft ist es dringend notwendig, die Ausnahmen des *sui generis*-Rechts zu erweitern.[149]

Einen Schritt in die richtige Richtung geht die Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt[150]: Der Ausnahmekatalog des *sui generis*-Rechts soll danach um eine zweigleisige *Text-* und *Data-Mining*-Schranke[151] erweitert werden: Text- und Data-Mining-Aktivitäten zum Zwecke der wissenschaftlichen Forschung sind nach Art. 3 DSM-RL freizustellen, soweit sie durch Forschungsorganisationen oder Einrichtungen des Kulturerbes[152] ausgeführt werden. Für sonstige Text- und Data-Mining-Aktivitäten gilt die engere Ausnahme in Art. 4 DSM-RL: Sie ist nur anwendbar, wenn die Datenbankhersteller ihre Datenbanken nicht ausdrücklich und in angemessener Weise mit Nutzungsvorbehalten versehen, Art. 4 Abs. 3 DSM-RL.

Die Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt sieht zudem in Art. 5 eine Schranke für den digitalen Unterricht vor.[153] Anders als die allgemeine Schranke für den Unterricht in Art. 9 lit. c Alt. 1 DB-RL stellt Art. 5 DSM-RL für den digitalen Unterricht nicht nur die Entnahme, sondern auch die Weiterverwendung frei. Dies ist zu begrüßen, denn eine Freistellung der Entnahme zur Veranschaulichung des Unterrichts bleibt ineffektiv, wenn

---

147 Art 9 lit a-c DB-RL. Vgl zur divergierenden Umsetzung in den einzelnen Mitgliedstaaten *JIIP*, Study (Fn 13) 10, 131 mwN sowie *JIIP*, Study (Fn 13) Annex 1: Legal Analysis, 87 f mwN.

148 Kritisch zu den engen Ausnahmen des *sui generis*-Rechts *Leistner*, Big Data (Fn 9) 27 (46-49).

149 Aus Platzgründen kann im Rahmen des Beitrags nicht ausführlicher auf alle konkret erforderlichen Erweiterungen der Ausnahmen des *sui generis*-Rechts eingegangen werden, s aber mit überzeugenden Vorschlägen *de lege ferenda Leistner*, Big Data (Fn 9) 27 (46-49). Im Rahmen der zweiten Evaluation der DB-RL plädierten nun ebenfalls zahlreiche Teilnehmer für eine Ausweitung der Ausnahmen, da diese zu eng gefasst seien, vgl *JIIP*, Study (Fn 13) 10, 58-60 mwN. Die Kommission stellte zwar abschließend fest, dass die Ausnahmeregelungen des *sui generis*-Rechts Probleme bereiten, „*significant data lock-up*"-Situationen seien aber nicht beobachtet worden, vgl SWD(2018) 147 endg, 20 f, 29 f mwN.

150 Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG (im Folgenden: DSM-RL), abrufbar unter https://data.consilium.europa.eu/doc/document/PE-51-2019-INIT/en/pdf.

151 Vgl Art 3 und Art 4 DSM-RL sowie Erwägungsgründe 5, 8, 9-18.

152 Vgl zur Legaldefinition dieser beiden Begriffe Art 2 Nr 1, 3 DSM-RL.

153 Vgl ferner Art 6 DSM-RL, der Vervielfältigungen zugunsten des Erhalts des Kulturerbes freistellen und ebenfalls auf das *sui generis*-Recht Anwendung finden soll. Weitere Ausnahmen sieht nun Art 3 der Richtlinie 2017/1564/EU über bestimmte zulässige Formen der Nutzung bestimmter urheberrechtlich oder durch verwandte Schutzrechte geschützter Werke und sonstiger Schutzgegenstände zugunsten blinder, sehbehinderter oder anderweitig lesebehinderter Personen und zur Änderung der Informationsgesellschaft-Richtlinie v 13.10.2017, ABl L 242, 6 vor, vgl dazu insgesamt SWD(2018) 145 endg, 43 mwN; *JIIP*, Study (Fn 13) 18, 80 mwN.

die Weiterverwendung verboten bleibt.[154] Dementsprechend sollte zumindest die Ausnahme in Art. 9 lit. b Alt. 1 DB-RL *de lege ferenda* ebenfalls die Weiterverwendung freistellen.[155]

3. Fazit

Sowohl die Datenbank- als auch die Trade-Secrets-Richtlinie entfalten im Kontext der Datenwirtschaft eine robuste Schutzwirkung. Die flexiblen Freistellungen der Trade-Secrets-Richtlinie können den Besonderheiten und Bedürfnissen der dynamischen datengetriebenen Wirtschaft angemessen Rechnung tragen, bedürfen aber der Konkretisierung. Der Ausnahmenkatalog des *sui generis*-Rechts ist hingegen zu eng und statisch gefasst. Zwar unternimmt die Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt erste – im Grundsatz begrüßenswerte – Schritte zur Anpassung der Ausnahmen an das digitale Zeitalter. Vor dem Hintergrund der weiten Schutzwirkung des *sui generis*-Rechts und den Besonderheiten und Bedürfnissen der Datenwirtschaft ist der Ausnahmekatalog aber grundlegend zu überdenken.[156]

Insgesamt bedarf es weiterer Forschung, ob über die bestehenden Freistellungen hinaus konkrete sektorspezifische Zugangs-, Nutzungs- und flankierende Informationsrechte etabliert werden sollten, um den freien Datenfluss im Interesse der Informationsfreiheit, der Innovation und der Transparenz zu fördern.[157]

C. Fazit und Ausblick: Vereinheitlichung und Reform statt Revolution

Der europäische Rechtsrahmen bietet bereits *de lege lata* eine Infrastruktur für den digitalen Strukturwandel in Gestalt von Big Data & Co. Einzeldaten sind zwar aus guten Gründen aus dem Schutzbereich des Datenbank- und Geheimnisschutzes ausgeklammert. Datensets (strukturiert und unstrukturiert, samt Metadaten), neuronale Netze, Algorithmen und deren Software-Implementierungen genießen aber regelmäßig weitreichenden Geheimnisschutz. Strukturierte Datensets sind in der Regel sogar kumulativ durch Datenbank- und Trade-Secrets-Richtlinie geschützt, solange und soweit sie relativ geheim bleiben. Mit Veröffentlichung verlieren sie zwar ihren Geheimnisschutz, bleiben aber weiterhin durch das *sui generis*-Recht geschützt. Damit begründet die Trade-Secrets-Richtlinie im Verbund mit der Datenbank-Richtlinie weitreichende Schutzrechte an sämtlichen schutzwürdigen und schutzbedürftigen Bestandteilen eines typischen Big

[154] Ebenso *Derclaye*, The Database Directive, in Stamatudē/Torremans (Hg) EU copyright law (Cheltenham, UK/Northampton, MA, USA 2014) 298 (337): „[… Art 9 lit b DB-RL is] in effect quasi unusable since to teach and research one almost always has to communicate to the public".

[155] Vgl dazu auch *JIIP*, Study (Fn 13) 59 f mwN; zur Frage, ob sich der einschränkende Passus „zur Veranschaulichung" auch auf Art 9 lit b Alt 2 DB-RL bezieht, vgl verneinend *JIIP*, Study (Fn 13) Annex 1: Legal Analysis, 39 mwN.

[156] Zu überdenken ist überdies die überlange Schutzdauer des *sui generis*-Rechts vgl dazu *Leistner,* Big Data (Fn 9) 27 (49 f mwN); vgl nun auch *JIIP*, Study (Fn 13) 80; *JIIP*, Study (Fn 13) Annex 1: Legal Analysis, 101 mit dem Vorschlag einer Verkürzung auf fünf Jahre, der sich an der vergleichbaren Rechtslage in Südkorea orientiert.

[157] Vgl zur DB-RL *Leistner*, Big Data (Fn 9) 27 (42-46 mwN); zur TS-RL *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (313 f mwN).

Data-Sachverhalts. Das Datenschutzrecht beschränkt diese Schutzrechte und kann damit den Rechten und Interessen der jeweils betroffenen Personen Rechnung tragen.[158] Damit lässt sich bereits *de lege lata* von einem „Europäischen Datenrecht" sprechen, das mit dem Datenbank-, Geheimnis- und Datenschutz auf drei tragenden Säulen ruht. Ergänzend können die Parteien im Rahmen ihrer Privat- und Parteiautonomie[159] flexible und einzelfallgerechte Anpassungen vornehmen.[160] Wer vor diesem Hintergrund für die Einführung neuer Schutzrechte[161] plädiert, trägt die Argumentations- und Begründungslast. Denn die Schöpfung und Zuweisung neuer Schutzrechte bedarf angesichts des bereits existenten „Europäischen Datenrechts" sowie wegen des damit verbundenen Eingriffs in die allgemeine Handlungs-, Wettbewerbs- und Informationsfreiheit[162] einer besonderen Rechtfertigung.[163] Im Vergleich dazu ist die Anpassung des bestehenden Rechtsrahmens ein milderes, jedenfalls gleich geeignetes, und damit vorzugswürdiges Mittel.[164] Es ist somit nicht erforderlich, den Kreis an Schutzrechten zu vergrößern, um dem digitalen Strukturwandel Rechnung zu tragen. Vielmehr sollte die Optimierung des bestehenden Rechtsrahmens in den Mittelpunkt der wissenschaftlichen Betrachtung gerückt werden. Denn dem Geheimnis-, Datenbank- und

---

158 Vgl allgemein *Specht*, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int 2017, 1040 (1042 ff). *Amstutz* und *Fezer* wollen die Rechte und Interessen der Individuen durch ein Ausschließlichkeitsrecht an den „Userdaten" (*Amstutz*) bzw. „verhaltensgenerierten Daten" (*Fezer*) schützen (vgl oben Fn 2). Beide tragen allerdings die Begründungslast: Warum ist die Schaffung eines solchen Ausschließlichkeitsrechts erforderlich? Mit dem Datenschutzrecht existiert bereits ein spezielles Instrument zum Schutz personenbezogener Daten. Soweit sich vor dem Hintergrund des begrenzten digitalen Strukturwandels ein erhöhter Schutzbedarf ergibt, könnte man beim Datenschutzrecht ansetzen und dieses überdenken bzw. verbessern. In diese Richtung zu Recht der Diskussionsbeitrag von *Thouvenin* zum Referat von *Amstutz* (AcP 218 (2018), 552 (554)); ähnlich bereits *Leistner*, Big Data (Fn 9) 27 (54). Zum Schutz des Individuums unter den Bedingungen automatischer Datenverarbeitung etwa bereits BVerfG NJW 1984, 419 (422) – Volkszählungsurteil (vgl dazu Fn. 7).

159 Zur nahezu weltweiten Anerkennung der schuldvertraglichen Parteiautonomie etwa allgemein *Basedow*, Theorie der Rechtswahl oder Parteiautonomie als Grundlage des Internationalen Privatrechts, RabelsZ 75 (2011), 32 (33 ff mwN zu den Ausnahmen).

160 Zum flexiblen vertragsrechtlichen Umgang mit Daten *Specht*, Rechtsvergleichende Analyse (Fn 2) 9 (40-47); allgemein zum evolutionären Potential des Rechts im Zusammenhang mit der Vertragsfreiheit *Herresthal*, Constitutionalisation of Freedom of Contract in European Union Law in Ziegler (Hg) Current Problems in the Protection of Human Rights (Oxford 2013) 89 (97).

161 S zu den vorgeschlagenen neuen Schutzrechten an Daten im Überblick A.

162 Umfassend zur grundrechtlichen Relevanz eines etwaigen Datenrechts *Wiebe*/*Schur*, ZUM 2017, 461 (462 ff mwN). Vgl dort auch die Ausführungen zu weiteren betroffenen Grundrechten in Gestalt der Berufsfreiheit und den Kommunikationsfreiheiten sowie des allgemeinen Gleichheitssatzes. Die Schaffung eines neuen Rechts an Daten ist zudem rechtfertigungsbedürftig, weil sie unnötigerweise weitere Konkurrenzprobleme provoziert, vgl Fn 166.

163 Aus ökonomischer Perspektive gibt es jedenfalls nach derzeitigem Kenntnisstand keine Gründe für die Schaffung neuer Schutzrechte an Daten, vgl nur *Kerber*, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int. 2016, 989 (997, 989); *Hugenholtz*, Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?, in: Lohsse/Schulze/Staudenmayer (Hg) Trading data in the digital economy: legal concepts and tools, (Baden-Baden 2017) 75 (80-81 mwN); differenzierend *Duch-Brown/Martins/Mueller-Langer*, The economics of ownership, access and trade in digital data, Joint Research Centre Digital Working Paper 2017-01, 23 ff, die auf die negativen wirtschaftlichen Auswirkungen abstellen, die durch die derzeit bestehende Rechtsunsicherheit im Hinblick auf die Rechte an Daten hervorgerufen wird. Es ist aber fragwürdig, ob die Schaffung neuer Recht an Daten zur Herstellung von Rechtssicherheit geeignet und erforderlich ist. Ein milderes und jedenfalls gleich geeignetes Mittel stellt die Optimierung des bestehenden Rechtsrahmens dar.

164 Zur maßgeblichen Bedeutung des Verhältnismäßigkeitsgrundsatzes *Wiebe*/*Schur*, ZUM 2017, 461 (469 mwN). Der Gesetzgeber verfügt freilich im Grundsatz über einen weiten Gestaltungsspielraum.

Datenschutzrecht gelingt es in einigen Bereichen nicht, für Rechtssicherheit zu sorgen und den Besonderheiten und Bedürfnissen der Datenwirtschaft gerecht zu werden:[165]

Besondere Probleme bereitet die Bestimmung der Inhaberschaft eines Geschäftsgeheimnisses bzw. eines *sui generis*-Rechts. Rechtssicherheit können die Beteiligten nur erzielen, indem sie privatautonome Vorkehrungen treffen. Flankierend sollte ein Geheimnis- und Datenbankschutzregister etabliert werden. Mit dessen Hilfe ließen sich Rechte an Geschäftsgeheimnissen und Datenbanken rechtssicher, geheimniswahrend und transaktionskostensparend dokumentieren, lizenzieren und übertragen.

Überdies ist die Schutzwirkung des Datenbank- und Geheimnisschutzes an die Besonderheiten und Belange der Datenwirtschaft anzupassen. Im Rahmen der Trade-Secrets-Richtlinie eröffnet die Verwendung einer Vielzahl unbestimmter Rechtsbegriffe und die einzelfallbezogene Verhältnismäßigkeitsprüfung auf Durchsetzungsebene hierfür einen breiten Spielraum. Zudem sichert die Trade-Secrets-Richtlinie im Interesse von Informationsfreiheit, Innovation und Wettbewerbsförderung wichtige Freiräume. Um Rechtssicherheit zu schaffen, sollten die zahlreichen Generalklauseln und Freistellungen allerdings vor dem Hintergrund typischer Big Data-Konstellationen konkretisiert werden. Der Ausnahmenkatalog des *sui generis*-Rechts ist dagegen zu eng gefasst. Zwar unternimmt die Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt erste Schritte zur Anpassung der Ausnahmen an das digitale Zeitalter. Vor dem Hintergrund der weiten Schutzwirkung des *sui generis*-Rechts und angesichts der Besonderheiten des digitalen Zeitalters ist der Ausnahmekatalog aber grundlegend zu überarbeiten. Insgesamt bedarf es weiterer Forschung, ob über die bestehenden Freistellungen hinaus konkrete sektorspezifische Zugangs-, Nutzungs- und flankierende Informationsrechte etabliert werden sollten.

Zudem ist es dringend erforderlich, das Verhältnis des Datenbank-, Geheimnis- und Datenschutzes zueinander sowie zu sonstigen Schutzinstrumenten rechtlicher oder faktischer Art zu bestimmen.[166] Denn eine unkoordinierte Schutzrechtskumulation birgt die Gefahr, dass die Wertungen einzelner Schutzinstrumente konterkariert werden.[167] *De lege lata* versuchen sowohl Datenbank- als auch Trade-Secrets-Richtlinie das Verhältnis zu anderen Rechtsinstrumenten zu klären, indem sie einen pauschalen Vorbehalt zugunsten der Anwendbarkeit sonstiger einschlägiger Regelungen aussprechen.[168] Dieser pauschale Vorbehalt sollte *de lege ferenda* konkretisiert werden. Dabei sind

---

[165] Vgl für das Datenschutzrecht *Specht*, GRUR Int 2017, 1040 (1042 ff mwN).

[166] Auch bei Schaffung eines neuen Rechts an Daten wäre namentlich der bereits bestehende Schutzumfang qua Datenbank-, Geheimnis- und Datenschutz zu klären, um das Konkurrenzverhältnis des neuen Rechts zu den bestehenden Schutzinstrumenten bestimmen zu können. Allgemein zu den „disruptive overlaps", die ein neues Recht an Daten provozieren würde *Hugenholtz*, Data Property (Fn 162) 75 (90-94, 96-97 mwN).

[167] Allgemein zu den Problemen, die aus sich überlagernden Schutzinstrumenten resultieren: *Derclaye*/*Leistner*, Intellectual Property Overlaps (Oxford 2011); *Leistner*, Konsolidierung und Entwicklungsperspektive des Europäischen Urheberrechts (Bonn 2008) 50 ff.

[168] Vgl Art 13 DB-RL, Art 1 Abs 2, Erwägungsgründe 37-39 TS-RL.

die relevanten Rechtsgebiete im Rahmen eines kohärenten Gesamtkonzepts sorgfältig miteinander abzustimmen.[169] Besonders bedeutsam ist dabei die Interaktion des Datenbank- und Geheimnisschutzes mit dem Datenschutzrecht.[170] Denn der Anwendungsbereich des Datenschutzrechts ist im Rahmen typischer Big Data-Sachverhalte regelmäßig eröffnet: Erstens ist der Kreis personenbezogener Daten weit zu ziehen.[171] Zweitens lässt sich die Unterscheidung zwischen Personen- und Sachdaten immer weniger durchhalten:[172] Mithilfe von Big Data-Analysen ist es vielfach möglich, selbst bei vermeintlich neutralen Sachdaten einen Personenbezug (wieder-)herzustellen.[173]

Schließlich drohen wegen des differenzierenden Harmonisierungskonzepts erheblich divergierende nationale Geheimnisschutzregime zu entstehen, denen die Richtlinie gerade abhelfen wollte.[174] Die unterschiedliche Umsetzung der Datenbank-Richtlinie in den einzelnen Mitgliedstaaten hätte als abschreckendes Beispiel dienen sollen. Vor diesem Hintergrund sollte *de lege ferenda* zumindest in zentralen Bereichen eine Vollharmonisierung angeordnet werden.

Zudem ist zu bedenken, dass Sachverhalte im Kontext der Datenwirtschaft regelmäßig einen grenzüberschreitenden Bezug aufweisen. Daher wäre eine (weitergehende) internationale Vereinheitlichung des Datenbank- und Geheimnisschutzes wünschenswert.[175] Geheimnisbegriff und

---

[169] Aus Platzgründen kann im Rahmen des Beitrags nicht näher hierauf eingegangen werden. Zu den internen und externen Konkurrenzen im Rahmen der DB-RL *Leistner*, Big Data (Fn 9) 27 (51-54). Zum Verhältnis von Geheimnis- und Datenschutz *Radoń*, Trade Secrets Protection for 'Big Data' (München 2015) 59 mwN; *Gianclaudio*, Trade Secrets v Personal Data: a possible solution for balancing rights, IDLP 2016, 102 ff mwN; *Picht*, Dateneigentum und Datenzugang, Jusletter IT 11 Dezember 2017 (Rz 8 f); allgemein zum Verhältnis des Datenschutzrechts zu zivilrechtlichen Rechtspositionen an Daten *Specht*/*Jannik*, Considering the relationship between the civil law treatment of data and data protection law in Germany, JIPLP 2018, 504 (506 f, 511 f); zum Verhältnis von Geheimnis- und Datenbankschutz vgl SWD(2018) 147 endg, 43 f sowie *JIIP*, Study (Fn 13) 88-91. Zum Verhältnis von lauterkeitsrechtlichem Leistungs- und Geheimnisschutz vgl *Becker*, Rechte an Daten – Industrie 4.0 und die IP-Rechte von morgen, JZ 2017, 936 (947 ff); zu den kartellrechtlichen Grenzen des Geheimnisschutzes vgl *Witz*, Grenzen des Geheimnisschutzes in Büscher/Erdmann/Haedicke et al (Hg) Festschrift für Joachim Bornkamm zum 65. Geburtstag (München 2014) 513 (514 ff).

[170] Zu dem Begriff der Kommunikationsdaten *Specht*, Rechtsvergleichende Analyse (Fn 2) 9 (14, 16 f mwN); *Czychowski/Siesmayer* in Kilian/Heussen (Hg) Computerrechts-Handbuch (34. Aufl. München 2018) Teil 20.5 (Rn. 18).

[171] *Dreier* in Dreier/Schulze UrhG (2018) Vorbemerkung §§ 87a ff Rn 13 mwN; *Schweitzer*/*Peitz*, NJW 2018, 275 (278 mwN); *Specht*, Rechtsvergleichende Analyse (Fn 2) 9 (14-16 mwN).

[172] Vgl *Drexl*, NZKart 2017, 415 (416); *Wiebe*/*Schur*, ZUM 2017, 461 (462).

[173] *Mayer-Schönberger*/*Cukier*, Big Data (Fn 36) 13 ff mwN und zahlreichen Beispielen; zu weiteren denkbaren Fällen vgl *Sattler*, Allgemeiner rechtlicher Rahmen (Fn 95) 27 (30); *Drexl*, NZKart 2017, 415 (416) verweist zudem zu Recht darauf, dass aufgrund zufälliger Korrelationen zwischen verschiedenen Daten Rückschlüsse auf Einzelpersonen möglich werden; vgl auch die Stellungnahme des *Europäischen Datenschutzbeauftragen*, Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von „Big Data" (Brüssel 2014) 8, 13 mwN, abrufbar unter https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en. Zur Forderung, rechtssichere Möglichkeiten zur Beseitigung des Personenbezugs zu etablieren, s *Specht*, Rechtsvergleichende Analyse (Fn 2) 9 (85 mwN).

[174] Vgl dazu bereits *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (316); vgl jüngst ähnlich *EUIPO*, The Baseline of Trade Secrets Litigation in the EU Member States (Alicante 2018) 8. Vgl nun bspw zur Umsetzung in Deutschland Fn 44.

[175] Für den Datenbankschutz *Leistner*, Big Data (Fn 9) 27 (50); für den Geheimnisschutz *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (317 mwN).

Struktur der Verletzungshandlungen sind jedenfalls international anschlussfähig.[176] Versuche, das *sui generis*-Recht im Rahmen einer internationalen Konvention zu etablieren, dürften allerdings erfolglos bleiben, solange sich die USA nicht zur Verabschiedung eines entsprechenden nationalen Schutzregimes entschließen.[177] Dort sind zahlreiche entsprechende Gesetzgebungsvorhaben[178] bislang gescheitert. Hauptgrund waren die Bedenken, durch die Einführung eines *sui generis*-Rechts würde ein mittelbares Eigentumsrecht an Daten geschaffen.[179]

Im Sinne des Tagungstitels – Strukturwandel und Privatrecht – bleibt damit festzuhalten: Das private „Europäische Datenrecht" kann dem begrenzten digitalen Strukturwandel in Gestalt von Big Data & Co. angemessen Rechnung tragen. Dafür müssen die bestehenden Schutzinstrumente allerdings im Rahmen eines kohärenten und international anschlussfähigen Gesamtkonzepts optimiert und aufeinander abgestimmt werden. Der Fokus darf dabei nicht einseitig auf den Belangen der Datenwirtschaft liegen.[180] Denn der digitale Strukturwandel bringt nicht nur neue wirtschaftliche Wertschöpfungschancen mit sich, sondern birgt auch erhebliche Risiken für die Rechte und Interessen der Individuen.

[176] *Sagstetter*, Big Data und der europäische Rechtsrahmen (Fn 5) 285 (317 mwN).

[177] *Dreier* in Dreier/Schulze UrhG (2018) Vorbemerkung §§ 87a ff Rn 12. Der Datenbankschutz im US-Amerikanischen Recht bezieht sich *de lege lata* nur auf Datenbanken mit schöpferischem Charakter vgl *Specht*, Rechtsvergleichende Analyse (Fn 2) 9 (33 f mwN). Zur Vorreiterrolle der USA in der Entwicklung der digitalen Ökonomie *Kerber*, Rechte an Daten in der digitalen Ökonomie (Fn 5) 115 (192).

[178] Vgl dazu *Gaster* in Sieber/Hoeren/Holznagel (Hg) Handbuch Multimedia Recht (München 2017) Teil 7.6 (Rn 233 ff mwN); *Mattioli*, Minn L Rev 2014, 535 (581 f).

[179] Vgl SWD(2018) 147 endg, 18, 39 mwN.

[180] Zu Recht kritisiert *Amstutz* vor diesem Hintergrund die bisherige Diskussion um die „(europäische) Datenwirtschaft", die andere soziale Dimensionen der Datenproblematik bislang weitgehend ausgeklammert hat, vgl *Amstutz*, AcP 218 (2018), 438 (441). Aus Platzgründen musste sich dieser Beitrag ebenfalls auf die ökonomischen Belange der Datenwirtschaft konzentrieren.