

„Dateneigentum“



Gliederung

- I. Untersuchungsgegenstand des Arbeitsgruppenberichts
- II. Übergeordnete Argumente
- III. Geltendes Recht: Schutzlücke?
- IV. Hypothetische Folgefragen eines „Dateneigentums“
- V. Fazit und Ausblick

I. Untersuchungsgegenstand des Berichts (1)

- Übergreifendes Ausschließlichkeitsrecht („Dateneigentum“)
- Daten „als solche“ => syntaktische Ebene
- Innerstaatlicher Ansatz (BGB)

I. Untersuchungsgegenstand des Berichts (2)

- Beschränkung auf Daten „als solche“ / „binäre Codes / „Menge von Zahlenreihungen“ / „syntaktische Informationen“ [teilw. auch „Rohdaten“ ↔ Maschinendaten; Industriedaten...]
 - *Inhaltsebene* und damit Diskussion um etwaige Vermögensrechte an *personenbezogenen* Daten ausgenommen (hier: Urheberrecht als Vorbild?; dazu etwa *Schwartmann/Hentsch*, RDV 2015, 221; zum Verhältnis etwaiger Datenrechte zum Datenschutzrecht *Specht*, GRUR Int. 2017, 1040); Abgrenzung auch von Rechten am *Datenträger*
 - *Persistent* (↔ *transient*) und *digital* (↔ *analog*)
 - Bestimmte Echtzeitdaten weisen ebenfalls großen wirtschaftlichen Wert auf

I. Untersuchungsgegenstand des Berichts (3)

- Anknüpfung an „syntaktische“ Ebene *wirklich* zielführend?
 - Begründung für einen bloß syntaktischen Schutz nach Commission Staff Working Document SWD(2017) 2 final, S. 34, Fn. 157:

„As such ideas or information [encoded] benefit already from intellectual or industrial property rights. A potential new right on data should enable data-driven innovation by providing access to relevant data for subsequent analysis.“
 - Geht es nicht letztlich – auch bei Big Data & Co – immer um Information(ssplitter)?

I. Untersuchungsgegenstand des Berichts (4)

- Ein *übergreifendes* Ausschließlichkeitsrecht, das *alle* denkbaren Konstellationen erfassen soll
 - Daten aus Social Media, Industriesensoren, Fitness-Apps, autonomen Kfz, medizinischen Bereichen, Forschungsmessungen usw. *gleichermaßen?*
 - Höchst abstrakte Ausgestaltung ohne jedwede Kontur
 - Bzgl. Schutzbereich, Schrankenregelung sowie der interessengerechten Zuweisung der Inhaberschaft überhaupt sinnvoll möglich? => m.E. (-)

I. Untersuchungsgegenstand des Berichts (5)

- Alternative: Verschiedene, abgestufte Datenrechte schaffen?
 - Differenzierung etwa nach dem Vorgang der Datenerzeugung / der Datenart / sektorspezifisch?
 - Zwar grundsätzlich sachgerechter; aber: Hohe Komplexität, da stets Vorprüfung erforderlich
=> Rechtsunsicherheit; Transaktionskosten!
- BGB als angedachte Rechtsquelle
 - Nationaler Alleingang nicht sinnvoll und politisch problematisch (*free flow of data*-Initiative der KOM!)

II. Übergeordnete Argumente

- Pro „Dateneigentum“ an Daten als solche
 - Rechtssicherheit
 - Handelbarkeit der Daten als Gut
- Contra „Dateneigentum“ an Daten als solche
 - Eingriff in Informations-, Nachahmungs- und Wettbewerbsfreiheit
 - Rechtliche Ausschließlichkeit kann Datenhandel und Innovation erschweren
 - Kein Marktversagen ersichtlich und Praxis fragt ein solches Recht nicht nach
 - Welchen konkreten Anwendungsfall möchte ein Ausschließlichkeitsrecht an Daten überhaupt absichern?
 - Datenmarkt (schon jetzt) und dessen Entwicklung (erst recht) undurchsichtig
 - Nationaler Alleingang in der Sache wenig sinnvoll und politisch problematisch (s.o.)
 - Anknüpfung an syntaktische Ebene von vorneherein fragwürdig (s.o.)

III. Geltendes Recht: Schutzlücke? (1)

- „Dateneigentum“ *de lege lata* (-)
 - Sacheigentumsregeln als Recht der körperlichen Gegenstände und der rivalen Nutzung (-), weder direkt noch analog, vom Rechtsgedanken her oder als Akzessorietätslösung
 - Hergebrachtes oder „neues“ existentes IP-Recht (-)
 - Schutzlücke nach geltendem Recht? (zugleich relevant für die **Frage eines Ausschließlichkeitsrechts *de lege ferenda***) => „bekannte Prüfung“ (jüngst etwa auch *BMVI*, „Eigentumsordnung“ für Mobilitätsdaten?, 2017, S. 46-60, vgl. auch S. 87 ff.)
 - Direkter Schutz nach § 823 Abs. 2 BGB i.V.m. §§ 303a, 202a ff. StGB; § 826 BGB, *aber jeweils Vorsatzerfordernis*

III. Geltendes Recht: Schutzlücke? (2)

- Mittelbarer Schutz (*de facto*-Schutz):
 - **Speichermedium:** Insbesondere § 823 Abs. 1 BGB (Eigentum; rechtmäßiger Besitz); Problem: Cloud
 - **Dateninhalt:** § 823 Abs. 1 BGB (sonstiges Recht: Recht am eingerichteten und ausgeübten Gewerbebetrieb; APR); § 823 Abs. 2 BGB i.V.m. § 17 ff. UWG (Know-how-Schutz) bzw. i.V.m. Datenschutzrecht, das *als solches* ebenfalls Schutz gewähren kann; Immaterialgüterrechte, v.a. Urheberrecht und hier v.a. § 4 Abs. 2 UrhG (Datenbankwerke), §§ 69a ff. UrhG (Softwareschutz), §§ 87a ff. UrhG (Investitionsschutz von Datenbanken)
- Was „fehlt“ im Arbeitsgruppenbericht?
 - Lauterkeitsrechtlicher Leistungsschutz? (abseits des „UWG-Nebenstrafrechts“ im Know-how-Bereich); weiterführend *M. Becker*, GRUR 2017, 346
 - Patentrecht => punktueller Schutz denkbar
 - zum Erzeugnisschutz von Videobilddaten: BGH, MMR 2013, 182 – MPEG-2; siehe jüngst BGH, GRUR 2017, 261 – Rezeptortyrosinkinase II; dazu *Zech*, GRUR 2017, 475
 - zur Patentfähigkeit einer Verbindung von Medienschutzdaten, die für ein Datenmedium spezifisch sind, mit Hauptdaten, die ein ursprüngliches Signal repräsentieren: BPatG, BeckRS 2012, 15425

III. Geltendes Recht: Schutzlücke? (3)

- Schutzlücke (?) bei fahrlässigem Datenzugriff durch Dritte bei Speicherung auf fremden Datenträger (Cloud)

=> Daten(-recht) als sonstiges Recht i.S.d. § 823 Abs. 1 BGB?

- Arbeitsgruppe wohl zu Recht (-); a.A. etwa *Spindler* und *G. Wagner*

⇒ Neues Schutzgesetz?

- Arbeitsgruppe zu Recht (-); a.A. etwa *Faust*

⇒ Neuer Deliktstatbestand?

- M.E. (-), a.A. *BMVI-Studie* zu Mobilitätsdaten, 2017

III. Geltendes Recht: Schutzlücke? (4)

- Vollstreckungsrecht: Ebenfalls keine Schutzlücke
 - Einzelzwangsvollstreckung
 - Daten = Vollstreckungsgegenstand: §§ 887 f. ZPO, mit Tendenz zu § 888 ZPO
 - Geldforderung = Vollstreckungsgegenstand, Daten = Vollstreckungsobjekt
 - Speichermedium, § 808 ZPO
 - „Anspruchsgesamtheit“ des „Dateninhabers“ als „anderes Vermögensrecht“ nach § 857 Abs. 1 ZPO
 - Erwägenswert: Unpfändbarkeit bei bestimmten Daten (Inhaltsebene!) gesetzlich (klarstellend) festschreiben
 - Insolvenz
 - Aussonderungsrecht nach § 47 InsO; Unpfändbarkeit?

IV. Hypothetische Folgefragen eines „Dateneigentums“

- Personelle Zuweisung (originärer Erwerb)
 - Verschiedenste Ansätze, z.B. Skripturakt (Strafrecht als Vorbild; unterschiedliches Verständnis bei Transformation ins Zivilrecht); Verkehrsanschauung; Investition in die Datenerzeugung...
- Gutgläubiger Erwerb von „Datenrechten“?
 - (-), mangels Rechtsscheinbestand
- Nicht eigens im Bericht behandelt, aber – zumal bei (abzuratenden!) „nationalen Alleingängen“ – von großer Relevanz:
 - Internationalzuständigkeits- und internationalprivatrechtliche Implikationen

V. Fazit und Ausblick (1)

- Keine Schutzlücke, kein Bedarf an „Eigentum“ an Daten „als solche“
 - Neues Ausschließlichkeitsrecht an *Dateninhalten*? => (-), zumindest kein übergreifendes „Super-IP-Recht“
 - Weiterentwicklung des Datenschutzrechts gen „Datennutzungsrecht“?
 - Diskussion um deliktischen Integritätsschutz bleibt virulent
- *Free flow of data*-Initiative der EU-KOM
 - EU-Lösung = Minimallösung
 - *Data Producer's Right* zwar zunächst erwogen
 - Tendenz geht aber zum Zugang, vgl. Art. 6, EG 5, 20 f. VO-Entwurf COM(2017) 495 final (dazu das Begleitdokument SWD(2017) 304 final, PART 1/2, 2/2) als *soft version* von Art. 20 DSGVO

V. Fazit und Ausblick (2)

- Daher im Ausgangspunkt: Beibehaltung des *status quo*: Faktische und / oder vertragsrechtliche Lösungen; als Korrektiv: AGB-Recht, Datenschutz- und Wettbewerbsrecht
- => möglicherweise aber Effektivierung der Korrekturmöglichkeiten
- Minimalinvasiver und gezielter Ansatz; weitere Studien zum Bedarf erforderlich! – Möglichkeiten:
 - Schaffung von Transparenz => prägnante Informationspflichten als Bestandteil eines Datenvertragsrechts, aber kein *information overload* => Datensouveränität => rot/gelb/grün-Plaketten/Piktogramme?

V. Fazit und Ausblick (3)

- Minimalinvasiver und gezielter Ansatz – Möglichkeiten (Fortsetzung):
 - AGB-Recht
 - Aber: Klauselkontrolle nur für Nebenleistungspflichten, greift also nicht, wenn Datenerhebung, -speicherung, -nutzung = Hauptpflicht
 - Typisierung der zugrunde liegenden Verträge => „Ausarbeitung eines dispositiven gemeineuropäischen Vertragsrechts für die Datenwirtschaft“? (*Drexl*, NZKart 2017, 415, 420)
 - Recht auf datenerhebungsfreie Produkte zur Stärkung der Datensouveränität (*M. Becker*, JZ 2017, 170)
 - Für bislang (vermeintlich) kostenlose Produkte wäre dann ggf. eine Geldzahlung fällig
 - EU-Standardvertragsklauseln

V. Fazit und Ausblick (4)

- „Datenzugangsrechte“ (Kontrolle und/oder Nutzung)
 - „Anti-Diskussion“
 - Zugangsrechte überwinden neben einer etwaigen rechtlichen auch die technische Exklusivität
 - Was ist das rechtlich? => Eher Regulierungsrecht
 - Kartellrecht; Datenschutzrecht: Auskunft (Art. 15 DSGVO) und Datenportabilität (Art. 20 DSGVO); nun auch bei nicht personenbezogenen Daten als Selbstregulierungsansatz erwogen: Art. 6 Vorschlag für eine VO über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der EU, COM(2017) 495 final
 - Sektorspezifische Ausgestaltung (siehe bereits Art. 6 VO [EG] Nr. 715/2007 bzgl. der Gewährung des Zugangs zu Kfz-Daten für unabhängige Marktteilnehmer; dazu jüngst OLG Frankfurt a.M., GRUR-RR 2017, 231)

Bei alledem gilt: Erst was man *wirklich* versteht, sollte man auch legislativ angehen...

=> Resultat der Arbeitsgruppe auch vor diesem Hintergrund überzeugend

=> Forschung im Grundlagenbereich, empirische Studien, Abwarten auf einschlägige Rechtsprechung 17 sollten zunächst das Mittel der Wahl sein...

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt: bjoern.steinroetter@iri.uni-hannover.de

Annex I: Art. 6 VO-Entwurf, COM(2017) 495 final

Artikel 6 Übertragung von Daten

(1) Die Kommission fördert und erleichtert auf Unionsebene die Entwicklung von Verhaltensregeln für die Selbstregulierung, um Leitlinien für bewährte Verfahren zur Erleichterung des Anbieterwechsels aufzustellen und damit die Anbieter beruflichen Nutzern vor Abschluss eines Vertrags über die Datenspeicherung und -verarbeitung hinreichend ausführliche, eindeutige und transparente Informationen in Bezug auf folgende Fragen geben:

- a) die Prozesse, technischen Anforderungen, Fristen und Entgelte, die für einen beruflichen Nutzer gelten, der zu einem anderen Anbieter wechseln oder Daten zurück in seine eigenen IT-Systeme übertragen möchte; dies umfasst auch die Prozesse und den Ort von Datensicherungen, die verfügbaren Datenformate und -träger, die erforderliche IT-Konfiguration und die Mindestnetzbandbreite, die Vorlaufzeit vor Beginn des Übertragungsprozesses und die Zeitspanne, in der die Daten für eine Übertragung verfügbar bleiben, sowie die Garantien für den Zugang zu den Daten im Falle der Insolvenz des Anbieters;
- b) die betrieblichen Anforderungen für den Anbieterwechsel oder die Übertragung von Daten in einem strukturierten, gängigen und maschinenlesbaren Format, die dem Nutzer für den Wechsel oder die Übertragung der Daten genügend Zeit lassen.

(2) Die Kommission hält die Anbieter dazu an, die in Absatz 1 genannten Verhaltensregeln innerhalb eines Jahres nach dem Beginn der Anwendung dieser Verordnung wirksam umzusetzen.

(3) Die Kommission überprüft die Entwicklung und wirksame Anwendung solcher Verhaltensregeln und die tatsächliche Bereitstellung von Informationen seitens der Anbieter spätestens zwei Jahre nach dem Beginn der Anwendung dieser Verordnung

Annex II: *BMVI*, § 823a BGB-Entwurf Schädigung von Daten

Wer vorsätzlich oder fahrlässig rechtswidrig Daten Dritter löscht, unterdrückt, unbrauchbar macht oder verändert ist dem Verfügungsberechtigten der Daten zum Ersatz des daraus entstehenden Schadens verpflichtet. Verfügungsberechtigter der Daten ist, wer bei wirtschaftlicher Betrachtungsweise für die Erstellung und Speicherung des Datums verantwortlich ist. Dies ist derjenige, der bei einer wirtschaftlichen Gesamtwürdigung des Erstellungsvorgangs die wesentliche Investition in die Datenerstellung vornimmt. Von einer wesentlichen Investition kann in der Regel ausgegangen werden, wenn eine unmittelbare Investition in die Datenerstellung vorgenommen wird, die Investition für den Vorgang der Datenerstellung von entscheidender Bedeutung ist und die getätigte Investition nicht schon anderweitig kompensiert worden ist. Indizien für eine Investition in diesem Sinne sind die wirtschaftliche Unterhaltung des datengenerierenden Gegenstandes, die Vornahme oder Initiierung der datengenerierenden Handlung sowie das Sacheigentum am datengenerierenden oder datenspeichernden Gegenstand.