Continental
The Future in Motion

Regensburger Verbund für Werbeforschung

Daten

„Eigentum“ und „Nutzungsrechte“

Prof. Dr. Jörg Fritzsche
Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht

Fakultät für Rechtswissenschaft

Universität Regensburg

1

Gliederung

I. Einführung
II. Rechtliche Regelung zu Daten
III. Dateneigentum?
IV. Zuordnung ohne „Dateneigentum“
V. Nutzungsrechte an Daten
VI. Nutzung personenbezogener/-beziehbarer Daten
VII. Fazit

2

Das „Datenthema“ – eine Auswahl

- Justizministerkonferenz
  - Arbeitsgruppe „Digitaler Neustart“ / Frühjahrkonferenz 2015
- Fachzeitschriften
  - Braucht das BGB ein Update?
    - Artikel von Michael Liepin und Dr. Gero Götz, NJW-aktuell 32/2016 und MMR-Aktuell 2016, 379185.
  - Ein Update für das Zivilrecht
    - Artikel von Eva Lux und Michael Liepin, NJW-aktuell 32/2017.
  - The Consequences of Digitalization for German Civil Law from the National Legislator’s Point of View
    - Dr. Andreas Christians und Michael Liepin, Zeitschrift für Geistiges Eigentum, Band 9, 2017, S. 331-339
- Fachtagungen ohne Ende, z.B.
  - Zivilrechtslehrertagung 2017, GRUR-Jahrestagung 2018, ZfPW-Forum 2018

3

Rechtliche Regelungen zu Daten

4

Daten als Gegenstand gesetzlicher Regelung

- „klassisches“ Datenschutzrecht
  - DSGVO seit 25.5.2018
    - Art. 2 I DSGVO: … gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.
    - Art. 1 I DSGVO: Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten
  - ergänzend BDSG, LDSGe
  - Sonderregelungen u.a. zu
    - Daten bei Telemediendiensten (TMG), Personalakten, etwa §§ 116 ff. BDSG
- Schutz von Daten als Wirtschaftsgut („Big Data“)
  - keine direkte Regelung
  - indirekter Schutz über verschiedene Regelungen möglich

5

Schutz des Wirtschaftsguts „Daten“

- BGB: kennt keine Daten
  - historische Entwicklung, Gesetz von 1896
  - Regelungen zu Sachen in §§ 90 ff. BGB + im 3. Buch Sachenrecht
- Sachen = körperliche Gegenstände, § 90 BGB
  - Daten = nicht körperlich → keine Sachen
  - indirekter Schutz bei Verkörperung in Sachen
  - z.B. bei Datenverlust infolge Beschädigung von Datenträgern

  → Schadensersatz nach § 823 I BGB wg. Eigentumsverletzung am Datenträger
    - umfasst alle Schäden
    - also auch aus Datenverlust, z.B. Wiederherstellungskosten, Gewinnentgang
  - Problem: Datenverlust von Fremdserver/Cloud
    - Fehler des Diensteanbieters → in der Regel vertragliche Haftung
    - Schädigung durch Dritte: SchE allenfalls bei Beschädigung des Fremdservers
    - Drittschadensliquidation durch Serverbetreiber

6

Schutz des Wirtschaftsguts „Daten“ (2)

- andere Ansatzpunkte für Rechtsschutz über § 823 II BGB
  - Schadensersatz bei Verletzung von Schutzgesetzen
  - ggf. Unterlassung und Beseitigung analog § 1004 Abs. 1 BGB
- § 202a StGB: Ausspähen von Daten

  (1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

  (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.
- § 202b StGB: Abfangen von Daten

  Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

7

Schutz des Wirtschaftsguts „Daten“ (3)

- § 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten

  (1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
  1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
  2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

  herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. […]
- § 303a StGB: Datenveränderung

  (1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

  (2) Der Versuch ist strafbar.

  (3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

8

Schutz des Wirtschaftsguts „Daten“ (4)

- § 303b StGB: Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) (Versuchsstrafbarkeit)

(4) (besonderes schwere Fälle: 1. Vermögensverlust großen Ausmaßes, 2. gewerbs- oder bandenmäßiges Handeln, 3. Gefährdung der Versorgung der Allgemeinheit bzw. der Sicherheit der BRD)

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

Schutz des Wirtschaftsguts „Daten“ (5)

- § 17 UWG (wird bald ersetzt)

(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs … [wie Abs. 1]

1. sich ein Geschäfts- oder Betriebsgeheimnis durch
   a) Anwendung technischer Mittel,
   b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder
   c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist,

   unbefugt verschafft oder sichert oder
2. ein Geschäfts- oder Betriebsgeheimnis, das er … sich … unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. .

Schutz des Wirtschaftsguts „Daten“ (6)

- statt § 17 UWG ab 2018
  - Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung
    - Umsetzungsfrist für RL: 9.6.2018
    - RL gilt daher ggf. bereits jetzt unmittelbar, soweit > §§ 17 ff. UWG
- § 2 Nr. 1 GeschGehG-E:
  - Geschäftsgeheimnis = eine Information, die
    - a) weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und
    - b) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist;
- § 3 GeschGehG-E: eigenständige Nachschaffung erlaubt
  - Dritte dürfen solche Daten selbst erheben/sammeln

Schutz des Wirtschaftsguts „Daten“ (7)

- § 4 GeschGehG-E: Handlungsverbote

(1) Ein Geschäftsgeheimnis darf nicht erlangt werden durch

1. unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder
2. jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht.

(2) Ein Geschäftsgeheimnis darf nicht nutzen oder offenlegen, wer

1. das Geschäftsgeheimnis durch eine eigene Handlung nach Absatz 1
   a) Nummer 1 oder
   b) Nummer 2

   erlangt hat,
2. gegen eine Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt oder
3. gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen.

(3) Ein Geschäftsgeheimnis darf nicht erlangen, nutzen oder offenlegen, wer das Geschäftsgeheimnis über eine andere Person erlangt hat und zum Zeitpunkt der Erlangung, Nutzung oder Offenlegung weiß oder wissen müsste, dass diese das Geschäftsgeheimnis entgegen Absatz 2 genutzt oder offengelegt hat. […]

Universität Regensburg

Dateneigentum?

13

Universität Regensburg

Schutz des Wirtschaftsguts „Daten“ (7)

- ohne Eigentumsverletzung dennoch § 823 I BGB?
  - Verletzung „sonstiger Rechte“ – Daten?
    - Urheberrecht: in der Regel nicht
      - Daten als solch in der Regel keine persönliche geistige Schöpfung eines Menschen
      - insbesondere bei maschinengenerierten Daten
      - eventuell Schutz als Elemente einer Datenbank (§§ 87a ff. UrhG)
  - daher Frage nach „Dateneigentum“
    - Dateneigentum durch Analogie zu Sacheigentum und/oder Urheberrecht
      - verfassungsrechtliche Gründe dafür? Gleichbehandlung?
      - verschiedene Konstruktionen in der Diskussion (hier unerheblich)
    - Problem: Konstruktion eines Rechts an Daten (→ Immaterialgut!) geht wohl über eine richterliche Rechtsfortbildung hinaus
      - Immaterialgüterrechte werden durch Gesetzgeber determiniert
      - Schutzgut, Schutzvoraussetzungen, Schutzumfang usw.
      - vgl. Patentrecht, Urheberrecht, Designrecht, Markenrecht
      - also Eingreifen des [besser: EU-] Gesetzgebers notwendig

14

Universität Regensburg

Schaffung eines Rechts an Daten

- Dateneigentum → Monopolisierung von Daten
  - Problem der inhaltlichen Ausgestaltung
    - Schutz von was? → Begriff der Daten / unterschiedliche Erscheinungen
    - Schutzumfang und vor allem Schutzgrenzen
      - = Schranken zugunsten Dritter oder der Allgemeinheit (vgl. Urheberrecht)
  - Inhaberschaft des Datenerhebenden auch ohne Recht
    - auch hier: schutzwürdige Interessen Dritter an Datennutzung/-zugang
- heute: Tendenz gegen Notwendigkeit/Zweckmäßigkeit
  - Schaffung von „Dateneigentum“ durch Gesetzgeber nicht notwendig:
    1. wenn/weil hinreichender Schutz über andere existierende Regelungen
    2. weil Problem für Wirtschaft und Bürger eher: Zugang zu Daten
  - etwa Arbeitsgruppe Digitaler Aufbruch der JuMiKo
  - vgl. auch EU-Kommission, Mitteilung zum Aufbau eines gemeinsamen europäischen Datenraums, COM (2018)232 fin.

15

Universität Regensburg

Zuordnung ohne „Dateneigentum“

und „Zugangsrechte“

16

Reine Daten

- „reine Daten“ = hier: losgelöst von Personenbezug
- z.B. Messdaten von Fahrzeugen oder anderen Geräten
  - Rechtsprechung: Daten von Geschwindigkeitsmessanlage
    - Zuordnung zum Hersteller von Gerät oder Mess-Software?
    - dagegen OLG Naumburg ZD 2014, 628 wegen § 202a StGB:
    - Datenhersteller = wer den Vorgang steuert (hier Polizist)
  - Begründung über das Zivilrecht ohne„Dateneigentum“?
    - aber: Daten entstehen aus Gerätenutzung
    - § 100 BGB: Nutzungen:
      „Nutzungen sind die Früchte einer Sache oder eines Rechts sowie die Vorteile, welche der Gebrauch der Sache oder des Rechts gewährt.“
    - Früchte → § 99 BGB: nach bisheriger h.M. nur Sachen
      - anders bei „Rechtsfrüchten“ (z.B. aufgrund von Nutzungsrechten)
    - aber Daten aus Nutzung → Gebrauchsvorteile einer Sache

Reine Daten

- Daten als Gebrauchsvorteile i. S. v. § 100 BGB der Sache, die sie erzeugen
  - Gebrauchsvorteile stehen zunächst dem Eigentümer zu, § 903 S. 1 BGB
    - anders bei anderweitiger gesetzlicher Regelung
    - oder vertraglicher Vereinbarung
  - faktisch entstehen sie beim Benutzer der Sache
- faktisch oft nur dem Hersteller zugänglich, der die technische Herrschaft besitzt, die Daten abzurufen
  - m. E. problematisch, arg § 903 BGB insbesondere bei Kauf
  - Eigentumserwerb – umfassenden Herrschafts- und Nutzungsrecht
  - muss auch die Gebrauchsvorteile „Daten“ umfassen, sonst keine vollständige Vertragserfüllung
    - z.B. für Reparatur usw.
    - davon abgesehen: klassischer Datenschutz
  - Herstellerinteressen → transparente Regelung im Kaufvertrag
  - andere Unternehmen, die Daten nutzen wollen → Vertrag mit Hersteller

Recht auf Datennutzung / Datenzugang

und „Zugangsrechte“

Szenarien für Wunsch nach Zugang/Nutzung

- Drittanbieter benötigt Zugang vom „Dateninhaber“
  - z.B. unabhängige Kfz-Werkstätten oder Ersatzteilhersteller oder Zulieferer von Kfz-Herstellern
  - Ziel: Erbringung von Leistungen im Wertschöpfungsnetzwerk
- Zugang zu Datenpools mit dem Ziel
  - Eintritt in sonst unzugänglichen Dienstleistungsmarkt als neuer Wettbewerber des Dateninhabers
    - z.B. Suchmaschine will Zugang zu den gesamten Suchdaten von Google
    - eventuell Essential-Facilities-Doctrine, § 19 II Nr. 4 GWB
  - Nutzung für andere Zwecke / Eintritt in Markt ohne Wettbewerb zum Dateninhaber
    - z.B. Trainieren (selbstlernender) Algorithmen für diverse Verwendungsideen
    - Umwandlung Big Data → Smart Data
    - Interessen des Dateninhabers jedenfalls im Wettbewerb weniger tangiert

Rechtliche Ansätze für Datenzugangsrechte

- Vertragsrecht
  - immer denkbar und möglich, aber nur:
  - sofern Dateninhaber zum Abschluss von Verträgen über die entgeltliche Nutzung seines Materials bereit ist
- ohne Abschlussbereitschaft des Inhabers: Kartellrecht?
  - Missbrauchsverbot / essential facilities -Doktrin
    - Geschäftsverweigerung als Missbrauch / Behinderung
  - vgl. § 19 II Nr. 4 GWB: Zugang zu Infrastruktureinrichtungen
    - kaum wirkliches Fallmaterial
      - Ansätze EuGH C-418/01 – IMS-Health; C-170/13 Huawei/ZTE (aber Patent)
      - Suchmaschinenbetreiber wünscht Zugang zu gesamten Suchdaten von Google
  - vgl. § 19 II Nr. 1 GWB: Behinderung oder Diskriminierung
    - sachlicher Grund? keine Daten für Unternehmen außerhalb von Vertriebssystem etc.?

Zugang zu Daten via Kartellrecht

- Voraussetzung: marktbeherrschende Stellung
  - Frage des Einzelfalls, aber bei großen Datensammlern denkbar
  - Relevanz von Daten für Marktmacht insbesondere auf mehrseitigen Märkten, so § 18 IIIa Nr. 5 GWB
- oder Abhängigkeit, § 20 Abs. 1 S. 1 GWB?
  - Datennutzungswilliger könnte als Nachfrager vom (einzigen) Inhaber der erforderlichen Datenmenge abhängig sein
- eigentliches Problem:
  - Kriterien für berechtigte Nutzungsinteressen
  - Angemessenheit von Entgeltforderungen bei Überlassung
  - nur Einzelfallbetrachtung, wenig Allgemeingültiges

→ daher wohl spezielle (EU-) Datenregulierung zielführender

Recht auf Datennutzung / Datenzugang

und „Zugangsrechte“

Schutz personenbezogener Daten

- Exkurs?
  - nicht nur, da personenbezogene Daten zum Persönlichkeitsrecht der jeweiligen Person gehören
- Daten insbesondere von Fahrzeugen, Smartphones
  - Sammlung durch Hersteller von Geräten bzw. Apps
  - Personenbezug dieser Daten in der Regel herstellbar
  - str.:
    - Trennung von „Dateneigentum“ und „Recht an den eigenen Daten“ (→ Datenschutzrecht)? praktikabel möglich?
    - fast alle Daten personenbeziehbar → kein Nutzen der Unterscheidung
  - letztlich: Datensammlung erfordert Rechtfertigung, s. Art. 6 DSGVO

Artikel 6 Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

25

Einwilligung in AGB

- Einwilligung in Datenverarbeitung durch Klauseln
- AGB-Kontrolle
  - Einbeziehungskontrolle, § 305 Abs. 2 BGB
    - Hinweis auf AGB
    - Möglichkeit zumutbarer Kenntnisnahme
    - Einverständnis des Vertragspartners
    - keine überraschende Klausel
  - Inhaltskontrolle, §§ 307 ff. (bzw. hier meist § 307 Abs 1, 2) BGB
    - keine Benachteiligung entgegen den Geboten von Treu und Glauben
    - Transparenz !!!
    - sicherlich keine Klausel, die Datennutzung umfassend erlaubt inklusive jeder Übertragung an Dritte
    - keine Konstruktion einer Einwilligung anderer Nutzer von Auto / App 7 etc.
      - Einwilligung höchstpersönlich, nicht durch Dritten
      - Gefahr der Beschränkung der Eigentümerbefugnisse des Erwerbers
      - → teilweise Vereitelung des Vertragszwecks

26

Zusammenfassung

27

Zusammenfassung

- Dateneigentum als Recht existiert nicht
- Datenherrschaft verschafft faktisch ähnliche Position
- Problem wohl in Wirklichkeit:
  - vertragliche Datennutzungsrechte von Herstellern
    - Problem Verhandlungsasymetrien – AGB-Verwendung – AGB-Kontrolle
  - Zugangsrechte zu Daten für Erwerber von Produkten
    - für personenbezogene Daten → teilweise in DSGVO verwirklicht
  - Zugangsrechte für andere Unternehmen zur Etablikerung
    - neuer Produkte oder Dienstleistungen jenseits der Interessen des Dateninhabers
    - konkurrierender Produkte oder Dienstleistungen
    - sonstige Zwecke
  - Kartellrecht für Einzelfälle geeignet
  - generell: Regulierung nach Modell TKG, EnWG etc

28