Sektorale Daten-Governance-Systeme und horizontale Datenzugangsregeln

Prof. Dr. Wolfgang Kerber
(Universität Marburg)

Verbraucherrechtstage 2019
„Datenzugang, Verbraucherinteressen und Gemeinwohl“

Bundesministerium der Justiz und für Verbraucherschutz (BMJV)
Berlin, 12./13. Dezember 2019

1. Einleitung (1)

Meine Fragestellung:

- Analyse der Instrumente für Datenzugang/-governance und deren Ausgestaltungsmöglichkeiten

Vorgehensweise:

- Analyse von horizontalen Datenzugangsregeln: Vor- und Nachteile
- Analyse von sektoralen Datenzugangsregimen: Vor- und Nachteile
  + Beispiele: > Zugang zu Bankkontodaten (PSD2)
    > Zugang zu Daten im vernetzten Auto
- Problem der Gestaltung von gesamten Daten-Governance-Systemen
  + Governance von Daten, die mehr ist als Datenzugang
  + Technologie und technologischer Regulierung (Interoperabilität / Standards)

1. Einleitung (2)

Ziel- und Kriterienraster für Datengovernance-Regelungen

- Ziele: + Wettbewerb, Innovation, Konsumentenwohlfahrt
  + Schutz der Privatsphäre, (Cyber-)Sicherheit, (industriepolitische Ziele)
- Kriterien für Zugang zu Daten:
  + Vorteile für Wettbewerb / Innovation durch breitere Verwendung von Daten
  + Anreize für Datenproduktion/-qualität
  + Beteiligung an Produktion von Daten
  + Schutz von Privatsphäre (Datenschutz) und Geschäftsgeheimnissen …
- Ökonomische Perspektive:
  + Marktversagen? > Marktmacht-/Wettbewerbs-/Innovationsprobleme
    > Informationsasymmetrien/Rationalitätsprobleme
    > technolog. Standards / Interoperabilität …
    > Transaktionskosten, Vorteile von Datenaggregation
  + Förderung freiwilliger Lösungen oder regulatorische Lösungen?

2. Horizontale Datenzugangsregeln (1)

Wettbewerbsrecht:

- Verweigerung des Zugangs zu Daten als missbräuchliches Verhalten von Unternehmen mit Marktmacht (Marktbeherrschung / relative Marktmacht)
- verschiedene Probleme / Diskussion über Stärkung in 10. GWB-Novelle

Datenportabilitätsrecht (Art. 20 DSGVO)

- Datenzugang über Ausübung des Datenportabilitätsrechts von Konsumenten
- vielfältige Probleme

Direkte Datenzugangs-/portabilitätsrechte

- gesetzl. Datenzugangsrechte / Datenportabilitätsrechte für nichtpersbezog. Daten
- (Australien: consumer data rights, aber sektorspezifisch umgesetzt)

Vertragsrecht (inkl. AGB-Kontrolle), Unlauterkeitsrecht

- vielfältige Fragen, unklar wie dies entwickelt werden kann

Kombinationen möglich

+ bspw. für marktbeherrsch. Plattformen Portabilität von Nutzerdaten in Echtzeit und Interoperabilität mit Komplementärdiensten (K. Wettbewerbsrecht 4.0)

2. Horizontale Datenzugangsregeln (2)

Vorteile und Probleme horizontaler Lösungen

- theoretisch: allgemeine Regelung im Prinzip vorzuziehen
- aber: Problem der Notwendigkeit einer starken Differenzierung bzgl. Zweckmäßigkeit von Datenzugang schwierig bei horizontalen Lösungen
  - \+ auch horizontale Regeln mit allgemeinen Kriterien erlauben sehr wohl eine hoch ausdifferenzierte Anwendung (=> Bildung von Fallgruppen)
- wer wendet die Kriterien an?
  - \+ Rechtsdurchsetzungs-/Regulierungsbehörde? (Guidelines, …)
  - \+ Gerichte im Rahmen der privaten Rechtsdurchsetzung?

  => verschiedene horizontale Lösungen für verschied. Datenzugangsprobleme besser geeignet, aber auch Überlappungen und Kombinationen
- wichtige Probleme:
  - \+ was bedeutet Zugang? welche Rechte hat der Datenempfänger (nur für bestimmte Zwecke, mit anderen teilbar / kombinierbar / verkaufbar, in Echtzeit?)
  - \+ Datenzugangsrecht reicht oft nicht: zusätzlich einheitliche Datenformate, Schnittstellen / technische Standards, Interoperabilität

3. Sektorale Datenzugangsregelungen (1)

Beispiel 1: Zugang zu Bankkontodaten (2. Zahlungsdienste-RL / PSD2)

- Öffnung von Bankkontodaten für innovative neue Zahlungsdienstleister
- Ausgangsproblem: Bankkontodaten unter exklusiver Kontrolle von Banken, was den Markteintritt neuer Zahlungsdienstleister (Fintech) sehr erschwert
  - + Marktversagensproblem: lock-in von Bankkunden, nicht genügend (Innovations-)Wettbewerb im Bankenbereich
  - + primär innovationspolitische Zielsetzung: Zugang marktmachtunabhängig (gilt als Musterbeispiel für Anwendung von Open Data / Open Banking)
- umfassende Regulierung:
  - + Zugang zu Bankkontodaten/Zahlungsdienstleister: direkte Zahlungsauslösung
  - + mit techn. Regulierung: bspw. API, Herausbildung von Standards
  - + Sicherheitsregulierung: doppelte Authentifizierung von Bankkunden plus Zertifizierung von Dienstleistern
  - + Europäische Bankenaufsicht (EBA) als zuständige Regulierungsbehörde
- Frage: Führt dies zu intendierten Effekten, bspw. Förderung von innovativen Start-ups?

3. Sektorale Datenzugangsregelungen (2)

Beispiel 2: Zugang zu Daten im vernetzten Auto

- Ökosystem vernetzten Fahrens mit vielen neuen Services und Unternehmen
- "extended vehicle" Konzept: Übertragung aller Daten auf proprietären Server der Autohersteller mit der Konsequenz ihrer exklusiven Kontrolle über Daten und technischen Zugang zum Fahrzeug (Gatekeeper-Position im Ökosystem)
- ermöglicht Ausschließung von unabhängigen Serviceanbietern und Übertragung von Marktmacht auf Sekundärmärkte innerhalb des Ökosystems (bedroht Wettbewerb, Innovation, Konsumentenwahlfreiheit auf Sekundärmärkten)
- Frage nach Zugang von unabh. Serviceanbietern zu Daten bzw. Fahrzeug, um Autonutzern in Konkurrenz zu Autoherstellern innovative Leistungen anzubieten
- alternative Politikvorschläge eines "shared server" bzw. offene interoperable Telematikplattformen, die Gatekeeper-Position beseitigen würde (TRL 2017)
- zur Zeit offene regulatorische Diskussion auf der EU-Ebene über Notwendigkeit eines sektoralen Datenzugangsregimes für Daten im vernetzten Auto
- es existiert bereits Zugangsregime für techn. Info zum Schutz des Wettbewerbs für tradition. Reparatur- und Wartungs-DL (Kfz-Typenzulassungs-VO 2018/858)

3. Sektorale Datenzugangsregelungen (3)

Vorteile / Probleme von sektorspezifischen Datenzugangsregimen:

- sektorspezifische Regulierung erlaubt stärker massgeschneiderte Lösungen, insbes. bzgl. Art der Daten und wer Zugang zu Daten bekommen soll
- Möglichkeit der Setzung von ex-ante Regeln (statt nur ex-post Kontrolle)
- gleichzeitige integrierte Lösung von einheitlichen Datenformaten, technologischen Zugängen (bspw. API), Mindeststandards von (Cyber)Sicherheit, aber auch sektorspezifische Musterverträge, Regeln über Zugangsgebühren etc.
- Beispiel: PSD2
- Beispiel: Daten im vernetzten Auto
  (in Kfz-Typenzulassungs-VO bereits einheitliche Datenformate, Zugangsgebühren / Nichtdiskriminierung (FRAND-ähnlich), technologische Regulierung (OBD-Adapter mit Diagnosedaten), Regulierung / Zertifizierungslösungen für sicherheitsrelevante Reparaturen/Ersatzteile von unabh. Anbietern)
- Probleme sektoraler Datenzugangsregime:
  + nur für wenige wichtige Bereiche möglich; viele Probleme so nicht lösbar
  + wesentlich anfälliger für "regulatory capture" durch Interessengruppen

4. Von Datenzugangsregelungen zu Daten-Governance-Systemen (1)

Was kann man aus den sektoralen Datenzugangsregimen lernen?

(1) Notwendig ist Analyse der Funktionsfähigkeit eines gesamten Ökosystems

- es geht nicht nur um punktuelle Datenzugangsfragen zw. einzelnen Firmen
- Frage nach einer geeigneten integrierten Gesamtlösung

(2) Datengovernance umfasst auch die Frage, wer Kontrolle/Governance über die Daten eines Ökosystems haben soll

- Bankkontodaten: Banken oder Bankkunden?
  + historisch: Banken hatten exklusive Kontrolle
- Daten im vernetzten Auto: Autohersteller oder Autoeigentümer/-nutzer?
  + Autohersteller beanspruchen exklusive Kontrolle, aber alternative Lösungen möglich
- Frage der initialen Zuordnung von Verfügungsrechten / faktischer Kontrolle über Daten ist Teil des Datengovernanceproblems

  => es geht nicht nur um Zugangsrechte

4. Von Datenzugangsregelungen zu Daten-Governance-Systemen (2)

(3) Datengovernancelösungen sind immer verknüpft mit technologischen Lösungen bzgl. Verfügung/Zugang/Transfer von Daten sowie (Cyber-)Sicherheit

- Beispiel: Datengovernance im Ökosystem vernetzten Fahrens:
  - \+ exklusive Kontrolle der Daten durch Autohersteller durch "extended vehicle" Konzept; bei anderer technologischer Lösung (offene interoperable Telematikplattform) ergibt sich völlig andere Datengovernance-Situation
  - \+ exklusive Kontrolle des techn. Zugangs zum Fahrzeug
    - > Problem der Interoperabilität mit komplementären Leistungen (notwendig für "remote services")
    - > Standardisierte Schnittstellen könnte Interoperabilitätsproblem lösen und Wettbewerb/Innovation durch unabh. Serviceanbieter ermöglichen
    - > hierfür notwendig: (Cyber)Sicherheitslösungen, die direkten Zugang zu Fahrzeug erlauben (mit Zertifizierungslösungen)
- Beispiel PSD2: hier Datenzugang und Ermöglichung der Leistungserbringung durch umfassende techn. Regulierungen bzgl. Authentifizierung, technolog. Zugänge (API)/techn. Standards, Zertifizierung (einschl. Regulierungsbehörde)

5. Daten-Governance-Systeme (1): Zur grundlegenden Architektur

Daten-Governance-Systeme und ihre Architektur

- Governance von bestimmten, abgrenzbaren (digitalen) Ökosystemen, die aus einer Menge von Anbietern und Nutzern von (oft komplementären) Leistungen innerhalb des Ökosystems bestehen
- notwendig: Analyse der Funktionsfähigkeit dieser Ökosysteme
  + bzgl. Ziele (Wettbewerb, Innovation, Verbraucher- und Datenschutz etc.)
  + Analyse von Marktversagensproblemen (oft simultan mehrere Probleme)
- Frage nach adäquaten Regelrahmen (Ordnung / "market design") für Öko-systeme (einschl. Selbstregulierung / Koregulierung)
- Regelrahmen ist immer eine Kombination aus allgemeinen (horizontalen) Regeln (Wettbewerbs-, Vertrags/Verbraucherrecht, Datenschutz/Datenportabilität etc.) und speziellen (sektoralen) Regeln für die Ökosysteme
  + Kontinuum bzgl. Anteil von horizontalen und sektoralen Regeln (plus Analyse deren Zusammenwirkens)
  + zusätzlich: wie wird das Ökosystem definiert, und für welchen spezifischen Problembereich sollen sektorale Regelungen gemacht werden

5. Daten-Governance-Systeme (2): Daten und Technologie

- Governance von Daten: Gestaltungsdimensionen und -optionen
  - + Definition von geeigneten Rechtsbündeln an Daten (oft komplexere Rechtsbündel mit vielfältigen Nutzungsrechten besser als exklusive Kontrolle)
  - + Option: Verwendung von Datentreuhänderlösungen, die Nutzung bspw. nach FRAND- und/oder anderen Bedingungen sicherstellen (Bsp. Autodaten)
  - + Option: Data sandboxes / Datennutzung unter Aufsicht statt Datentransfer
  - + Option: spezifische Regeln über Anonymisierung (plus privacy by design)
- Governance von Technologie:
  - + technologisches Design beeinflusst Governance von Ökosystemen
  - + Technologische Standardisierung / Regulierung wichtig für
    - > Datenzugang/-portabilität: standardisierte Datenformate
    - > standard. techn. Schnittstellen für Konnektivität / Interoperabilität (bspw. API), insbes. auch für komplementäre Leistungen im Ökosystem
    - > (Mindest-)Standards für Sicherheit (Cybersicherheit / security by design), einschl. Zertifizierungslösungen (für Anbieter von komplem. Leistungen)

6. Zur institutionellen Frage der Kompetenz zur Ausgestaltung von Datenzugangsregeln und Daten-Governance-Systemen

Frage: Wer entscheidet über Datenzugangs- und Daten-Governance-Systeme?

- Wer soll konkret über die Vielzahl von spezifischen Regeln auf rechtlicher und technologischer Ebene entscheiden und diese auch an sich rapide verändernde technologische und ökonomische Veränderungen anpassen?
- letztlich: Gesetzgeber: "rules vs. standards"-Ansatz ("standards" mit Delegation von Regelsetzungskompetenzen an bestimmte Institutionen)
- Optionen:
  - \+ Gerichte
  - \+ (sektoral) spezialisierte Regulierungsbehörden?
  - \+ auf digitale Probleme spezialisierte Regulierungsbehörde mit Kompetenz, für viele Bereiche adäquate Datenzugangs-/governance-Lösungen zu etablieren? (vgl. "digital market unit" / Furman report)
  - \+ (Beteiligung von Stakeholdern / Selbstregulierung)
- Regelsetzung auf internationaler, europäischer oder mitgliedstaatlicher Ebene?
  - \+ neheliegend: direkt EU-harmonisiert oder EU-Rahmenregelungen

7. Weitere Perspektiven

- Entwicklung v. "treuhänderischen" Lösungen als neues Governance-Instrument:
  + für Datensets im Rahmen von Datenzugangslösungen für Unternehmen
  + Governance von personenbezogenen Daten von Individuen für Stärkung von Datensouveränität: privacy management tools / PIMS, neue Intermediäre im Interesse der Datensubjekte
    (vgl. Datenethikkommission / Komm. Wettbewerbsrecht 4.0)
- wichtig: mehr vorausschauende Analyse von Datengovernance-Problemen:
  + Datenzugangs/governance-Probleme nicht immer nur ex-post feststellen und dann reaktiv regulatorisch reagieren
  + oftmals stark pfadabhängige Prozesse, die schwer reversibel sind
  + soweit möglich auch vorausschauende Analyse und präventiver Ansatz (insbes. zur Verhinderung von (nicht-gerechtfertigten) Daten-Bottlenecks und daraus folgenden Gatekeeper-Positionen und Wettbewerbs- /Innovationsproblemen)