

## Datensouveränität und Recht 4.0

### Das Grünbuch „Digitale Plattformen“ im Spannungsfeld zwischen Datenschutz und Wettbewerbsrecht

Prof. Dr. Beatrix Weber, MLE

Institut für Informationssysteme, iisys, Hochschule für Angewandte Wissenschaften Hof

#### Einleitung

Das Grünbuch „Digitale Plattformen“ vom 30.05.2016 soll im Rahmen der Digitalen Strategie 2015 einen Ordnungsrahmen für mehr Investitionen und mehr Innovationen bei fairem Wettbewerb schaffen. Gleichzeitig sollen die Grundrechte und die Datensouveränität von Individuen und Unternehmen gesichert werden. Datenvermeidung kann nach dem Grünbuch in Zeiten von Big Data keine Leitlinie mehr sein.<sup>122</sup> Daten sind vielmehr der wichtigste „Grundstoff“ der digitalen Ökonomie. Zweckbindungsgrundsatz und Datensparsamkeit sind demnach konkretisierungsbedürftig und der Abwägung mit anderen Rechten und Interessen

nicht entzogen.<sup>123</sup> Ziel soll die effektive, individuelle Datensouveränität sein. Der Dateninhaber soll hierbei vor konkreten Missbrauchsgefahren geschützt werden.

Daten wird ein wirtschaftlicher Wert zugebilligt. Sie haben insofern die Funktion einer „neuen Währung“ und können als Substitut für ein Entgelt dienen.<sup>124</sup> Als Leitlinie zur Einwilligung in die Nutzung und Verarbeitung personenbezogener Daten wird im Grünbuch der vom „Unternehmen kommunizierte Zweck“ in den Mittelpunkt gestellt. Mehr Kommerzialisierung erfordere allerdings auch mehr individuelle Kontrolle. Eine Einwilligung nach Sphären, das sogenannte Identity Management, standardisierte Einwilligungen für bestimmte Geschäftsmodelle, Ampelsysteme, Zertifizierungen, die treuhänderische Wahrnehmung von Datenrechten durch Dritte und die Selbst- oder Koregulierung, z. B. durch Verhaltenskodizes, werden als mögliche Regelungsansätze angesprochen.<sup>125</sup> Datenanalyseverfahren, die individuelle Preisbildung und das Profiling werden bei vorheriger Einwilligung, die auf ausreichender Information basiert, als zulässig erachtet.<sup>126</sup>



#### Recht 4.0

*Notwendig ist die Koordinierung des gesamten Ordnungsrahmens, d. h. die Abstimmung der einzelnen Gesetze aufeinander mit Blick auf die übergeordneten Wertentscheidungen zu Innovation, Investition, Wettbewerb und Datenschutz bei digitalen Geschäftsmodellen, insbesondere unter Nutzung von Big Data.*

Recht 4.0 ist nicht nur Datenschutz bei der Nutzung von Big Data für digitale Plattformen. Datenschutz ist nicht nur BDSG oder Datenschutzgrundverordnung. Recht 4.0 ist der gesamte Ordnungsrahmen, der mit Blick auf Technologien digitaler Plattformen und die Nutzung von Big Data anzupassen und zu koordinieren ist. Im Grünbuch wird daher zu Recht auf den gesamten Rechtsrahmen verwiesen, der die Rechtsbeziehungen

der Marktteilnehmer regelt. Hierzu gehören neben der Datenschutzgrundverordnung u. a. das Gesetz gegen den unlauteren Wettbewerb (UWG), das Gesetz gegen Wettbewerbsbeschränkungen (GWB), das Telemediengesetz (TMG), das Urheberrechtsgesetz (UrhG) und das Telekommunikationsgesetz (TKG).

## Wettbewerbsrecht 4.0

### Regulierungsziel: Anwendung des Kartellrechts auf digitale Geschäftsmodelle

*Die Erweiterung der Marktkriterien auf unentgeltliche Leistungen führt im Ergebnis zur wirksamen Einbeziehung neuer digitaler Geschäftsmodelle, ist aber mit Blick auf die entgeltsubstituierende Funktion von „Daten“ und „Aufmerksamkeit für Werbung“ im Gesamtregulierungsrahmen nicht stringent.*

Die Anpassung des Kartellrechts an digitale Geschäftsmodelle wird mit dem Grünbuch und dem Referentenentwurf zur 9. GWB-Novelle aufgegriffen. Das Kartellrecht soll an den Strukturwandel unter Berücksichtigung der fortschreitenden Digitalisierung angepasst werden. Es soll aber kein branchenspezifisches Kartellgesetz begründet werden. Der Schutz und die Regulierungsfunktion des Kartellrechts sollen vielmehr sektorübergreifend bestehen bleiben. Im Sinne der nationalen Nachhaltigkeitsstrategie der Bundesregierung sollen Innovationspotenziale in Technologiemarkten geschützt und die Teilhabe möglichst vieler Wirtschaftsakteure (Unternehmen und Verbraucher) an dieser wirtschaftlichen Entwicklung gefördert werden.<sup>127</sup> Die Besonderheiten der digitalen Plattformen liegen u. a. in der häufigen Unentgeltlichkeit von Angeboten, Netzwerkeffekten und Konzentrationstendenzen, der Verarbeitung von Big Data, Lock-in-Effekten und einer hohen Dynamik technologischer Entwicklungen. Diese sind mit den herkömmlichen Marktdefinitionen des Kartellrechts häufig nicht adäquat zu erfassen.

Der **relevante Markt** wurde bisher räumlich durch ein geografisches Gebiet mit homogenen Wettbewerbsbedingungen und sachlich nach der Substituierbarkeit von Produkten und Dienstleistungen mit Blick auf Eigenschaften, Preis und Verwendungszweck abgegrenzt. Der Preis entfällt bei einer Vielzahl von unentgeltlich angebotenen Leistungen, die sich in den mehrseitigen Märkten der Internetökonomie u. a. durch Werbung finanzieren. Um hier eine Missbrauchskontrolle zu erreichen, soll nach § 18 Abs. 2a GWB-E die Unentgeltlichkeit von Leistungen einen Markt nicht mehr ausschließen. Diese Klarstellung scheint auf den ersten Blick digitale Geschäftsmodelle gut zu erfassen. Hinsichtlich des regulatorischen Gesamtvorhabens ist es allerdings nicht konsequent, auf der einen Seite den *Daten die Qualität eines Entgeltsubstituts zuzusprechen*<sup>128</sup>, andererseits aber für die Marktabgrenzung auf die Unentgeltlichkeit der Leistungen abzuheben. Auch die *Finanzierung über Werbung* beruht letztlich auf einem Entgelt für die Platzierung der Werbung oder die indirekte Einpreisung in ein Produkt. Die Änderung ist allerdings so konzipiert, dass die Unentgeltlichkeit keine marktausschließende Wirkung hat. § 18 Abs. 2a GWB-E: *„Der Annahme eines Marktes steht nicht entgegen, dass eine Leistung unentgeltlich erbracht wird.“* Insoweit wird das Ziel, die Besonderheiten der digitalen Geschäftsmodelle überhaupt zu erfassen, erreicht. Die Abgrenzung der entgeltlichen und unentgeltlichen Leistungen, die Zuordnung zu einem einheitlichen oder getrennten Markt und die Kriterien hierfür bleiben für die Rechtsanwendung offen. Sie sollen nach der Entwurfsbegründung der Einzelfallwürdigung überlassen bleiben,<sup>129</sup> was eine Rechtsunsicherheit für Unternehmen bedeutet.

### Regulierungsziel: Verhinderung von Lock-in-Effekten

*Das Regulierungsziel der Verhinderung von Lock-in-Effekten kann erreicht werden. Die Regelungen sind jedoch zur Herstellung von Rechtssicherheit für Unter-*



nehmen zu ungenau. Die Erfahrung in anderen Märkten zeigt, dass Rechtsstreitigkeiten über Jahre ein Investitions- und Innovationshemmnis darstellen.

Für die Bewertung der Marktstellung werden über § 18 Abs. 3 GWB hinaus in § 18 Abs. 3a GWB-E zusätzliche Kriterien eingeführt, mit denen die Besonderheiten digitaler Geschäftsmodelle berücksichtigt werden sollen: direkte und indirekte Netzwerkeffekte, parallele Nutzung mehrerer Dienste, Wechselaufwand (Kosten) für Nutzer, Größenvorteile durch Netzwerkeffekte, Zugang zu Daten und der innovationsgetriebene Wettbewerbsdruck.

**Indizien, die gegen einen Lock-in-Effekt**, d. h. gegen Marktzutrittsschranken, sprechen, sind damit die technische und auch tatsächliche Möglichkeit, mehrere Dienste oder Produkte nebeneinander zu nutzen (Multihoming), das Bereitstellen standardisierter Schnittstellen, die Erleichterung des Wechsels durch niedrige Wechselkosten und Datenportabilität. Die Kriterien der Heterogenität der Nutzer und der horizontalen Produktdifferenzierung der Plattformen sind lediglich in der Gesetzesbegründung des Referentenentwurfes genannt.<sup>130</sup> Nicht alle Kriterien stellen Besonderheiten digitaler Geschäftsmodelle dar. Daten als „essential facilities“<sup>131</sup> und der *diskriminierungsfreie Zugang zu Daten* sind als Kriterien nicht neu, sondern u. a. aus dem Automobil-Aftermarket im Zusammenhang mit der Bereitstellung technischer Informationen für markenungebundene oder Mehrmarkenreparaturbetriebe, sogenannte freie Werkstätten, geläufig.<sup>132</sup> Regelungen zur Erleichterung des Anbieterwechsels hinsichtlich Kostenfreiheit und Fristen sind aus dem Strom- und Gasmarkt<sup>133</sup> sowie dem Bereich der Telekommunikationsdienstleistungen<sup>134</sup> bekannt. Die Monopolkommission kritisiert in ihrem letzten Hauptgutachten hierzu die Beschränkung der Kriterien auf mehrseitige Märkte und Netzwerke und moniert die fehlende ausdrückliche Nennung in § 18 Abs. 3 GWB.<sup>135</sup>

Die Ausformung des Kriteriums des „**Zugangs zu Daten**“ wird für Unternehmen einer der Hauptfaktoren der Wirtschaftlichkeit ihrer digitalen Geschäftsmodelle werden. Die wirtschaftliche Bedeutung soll in einer Gesamtbetrachtung aller Umstände abhängig sein von

- Art und Umfang der vorhandenen Daten,
- ihrer Bedeutung für die Geschäftstätigkeit,
- den Fähigkeiten und Möglichkeiten des Unternehmens zur Datenauswertung und-verarbeitung,
- der Einschränkung der Möglichkeiten der Wettbewerber, vergleichbar große Datenpools aufzubauen,
- der exklusiven Herrschaft über bestimmte Daten,
- dem Zweck der Datenerhebung und-nutzung für das Unternehmen.

Unklar bleibt hierbei:

- Unter welchen konkreten Voraussetzungen erzeugt ein Datenbestand einen Lock-in-Effekt?
- Was heißt „übermäßiges Sammeln“ von Daten mit Blick auf die Nutzung von Big Data im Sinne einer Unausgewogenheit von Leistung und Gegenleistung?
- Mit welchem wirtschaftlichen Aufwand sind welche Daten in welchen Formaten zur Portierung bereitzustellen?<sup>136</sup>
- Wie sind sich verändernde Marktgegebenheiten mit Blick auf einen Lock-in-Effekt versus Innovationschutz für das Unternehmen zu bewerten?

### **Regulierungsziel: Fusionskontrolle von Start-up-Übernahmen**

*Das Ziel der Fusionskontrolle gesamtwirtschaftlich bedeutenderer Fälle für digitale Geschäftsmodelle wird erreicht. Angesichts der Höhe der Aufgreifschwelle ist die tatsächliche Lenkungsfunction fraglich. Eine Behinderung von innovativen Start-ups ist daher nicht zu erwarten.*

Mit der Einführung eines neuen Aufgreifkriteriums, des *Transaktionswertes*, soll die Fusionskontrolle bei der Übernahme von Start-ups ermöglicht werden, die ein hohes Marktpotenzial und für den Erwerber

eine hohe wirtschaftliche Bedeutung haben, die sich (noch) nicht in entsprechenden Umsätzen ausdrücken. Innovationen sollen geschützt und Märkte vor strukturellen Verschließungen bewahrt werden. Geringe Umsätze würden insbesondere im digitalen Wirtschaftsbereich nicht immer der wettbewerblichen Bedeutung des Unternehmens gerecht, da eine erfolgreiche Markteinführung mit einer großen Zahl von Nutzern und Netzwerkeffekten oft durch unentgeltliche oder preiswerte Angebote erreicht werde. Das Umsatzpotenzial entfalte sich oft erst nach der Übernahme, weswegen bereits etablierte Unternehmen mit internetbasierten Geschäftsmodellen versuchten, potenzielle Wettbewerber aufzukaufen.

Wenn die beteiligten Unternehmen weltweit insgesamt mehr als 500 Mio. Euro Umsatz erzielt haben, muss nur eines der beteiligten Unternehmen im letzten Geschäftsjahr vor dem Zusammenschluss Umsatzerlöse von mehr als 25 Mio. Euro erwirtschaftet haben. Die anderen Unternehmen dürfen im Inland Umsatzerlöse von 5 Mio. Euro nicht überschritten haben und mindestens eines muss im Inland tätig sein oder voraussichtlich tätig werden. Wenn dann der Transaktionswert (Kaufpreis zuzüglich etwaiger Verbindlichkeiten) mehr als 350 Mio. Euro beträgt, kann eine Fusionskontrolle stattfinden, siehe § 35 Abs. 1a, § 38 Abs. 4a GWB-E. Nach den im Referentenentwurf genannten Zahlen zu den wichtigsten Start-up-Übernahmen im letzten Jahr hätte nur eine Übernahme im einschlägigen Bereich gelegen. Für die Anwendung der Vorschrift werden daher auch nur Fälle im einstelligen Bereich erwartet.<sup>137</sup>

#### Datenschutz 4.0

##### „Dateninhaber“ als Datensouverän des persönlichen Gehalts und der wirtschaftlichen Verwertbarkeit der Daten

*Datensouveränität muss im Lichte des Rechts auf informationelle Selbstbestimmung und der digitalen Privat-*

*autonomie zwei Kernpunkte umfassen:*

- *die Hoheit über den persönlichen Gehalt der Daten und*
- *die Hoheit über die wirtschaftliche Verwertbarkeit.*

**Rechtlich relevante** Formen der Nutzung von Daten sind vor allem die Nutzung personenbezogener Daten sowie von Daten, die mit Rechten Dritter wie Urheberrechten, Rechten des Datenbankherstellers, Recht am eigenen Bild oder gewerblichen Schutzrechten verknüpft sind, Daten aus verschiedenen Quellen und das Sammeln zunächst unstrukturierter Datenmengen (data lakes), zumeist unter Nutzung großer Datenmengen (Big Data). Der Wert der Daten zur ökonomischen Nutzung steigt in der Regel mit der Menge der Nutzer und/oder der Granularität der Datenbestände. Die bisherigen Prinzipien des Datenschutzes kollidieren hier hinsichtlich Datensparsamkeit, Datenminimierung und kurzer Speicherdauer mit der Entwicklung innovativer Produkte und Dienstleistungen durch Nutzung von Big Data über längere Zeitreihen. „Volume“ (große Datenmengen), „Velocity“ (hohe Frequenz einströmender Daten) und „Variety“ (Mischung aus strukturierten und unstrukturierten Daten) sind zur Auswertung der Daten erforderlich.<sup>138</sup> Diese kollidierenden Rechte sind im Sinne einer Datability<sup>139</sup>, eines nachhaltigen und verantwortungsvollen Umgangs mit Daten, in Einklang zu bringen.<sup>140</sup>

Daten haben einen **ökonomischen Wert**. Sie können als Substitut für eine Zahlung behandelt werden, wenn sie als Entgelt in einem vertraglichen Austauschverhältnis dienen. Mit dem Vorschlag einer „**Richtlinie zu vertragsrechtlichen Aspekten bei der Bereitstellung digitaler Dienste**“<sup>141</sup> liegt ein erster Umsetzungsvorschlag zur rechtlichen Anerkennung der Funktion von Daten als **Entgeltsubstitut** vor. Diese liegt nach dem Richtlinienvorschlag bei aktivem Bereitstellen von Informationen wie Name, E-Mail-Adresse oder Foto vor. Cookies oder IP-Adressen, die nur anlässlich eines Kundenkontaktes eingesetzt oder erhoben werden,



sollen nach dem Entwurf kein Äquivalent für ein Entgelt darstellen, da sie nicht aktiv bereitgestellt würden. Das Abgrenzungskriterium der aktiven Bereitstellung erscheint fraglich, da sich hiernach nicht der ökonomische Wert von Daten bemisst. Dieser sollte aber Leitlinie zur Bestimmung eines potenziellen vertraglichen Austauschverhältnisses sein.

Unabhängig von der Diskussion der Einordnung des „Rechts an Daten“ oder „Rechts des Zugangs zu Daten“ als Inhaberschaft, Quasieigentum oder Leistungsschutzähnliches Recht<sup>142</sup> bleibt die Frage, wem die Entscheidung über die Verwertung, d. h. die wirtschaftliche Nutzung von Daten, zufallen soll: Kann der Einzelne im Sinne des Rechts auf informationelle Selbstbestimmung aktiv über die Nutzung seiner Daten bestimmen oder muss er im Sinne eines überwiegenden Schutzrechts vor dem Eingriff Dritter geschützt werden? Im Grünbuch wird hier eine deutliche Perspektive zur wirtschaftlichen Nutzung von Daten eingenommen. „Datensouveränität“ und „digitale Privatautonomie“ stärken die Stellung des Dateninhabers als Verfügungsbefugter über „seine“, insbesondere die personenbezogenen, Daten in Anlehnung an das Prinzip der Vertragsautonomie im deutschen Zivilrecht, das die Inkongruenz der Informationsstände und beherrschbaren Sphären für den Einzelnen durch besondere Verbraucherschutzrechte auflöst.

Die Hoheit über den persönlichen Gehalt der Daten erfordert wie beim Urheberrecht das Verbleiben eines **höchstpersönlichen, unveräußerlichen Kerngehaltes** beim Dateninhaber. Dieser Kerngehalt beinhaltet die Umkehrbarkeit bestimmter Entscheidungen zur Nutzung der Daten (Reversibilität)<sup>143</sup> wie das Recht auf Vergessen<sup>144</sup>, die Widerruflichkeit der Überlassung der Daten an Dritte, den Anspruch auf Information über die gespeicherten Daten und den Anspruch auf Löschung.<sup>145</sup> Im Übrigen stellt sich die Frage, ob das Nutzerverhalten großer Nutzergruppen von sozialen Medien wie Tinder, Instagram oder Snapshot ein wirk-

liches Schutzbedürfnis offenbart. Hier wird der Zugriff auf personenbezogene Daten und Bilder freiwillig einer Vielzahl von Nutzern gewährt. Teile des privaten Lebens und damit der Privatsphäre werden auf digitalen Plattformen gelebt. Wenn aber von einer Vielzahl von Nutzern Teile ihrer persönlichen Sphäre im Internet gelebt werden, sind personenbezogene Daten erforderlich. Die Prinzipien der Datensouveränität und der digitalen Privatautonomie erfordern, dieses Nutzerverhalten auf rechtmäßiger Basis möglich zu machen, unter Beachtung des unveräußerlichen Kerngehaltes der eigenen Daten.

Beide Bereiche, die Hoheit über den persönlichen Gehalt der Daten und die Hoheit über deren wirtschaftliche Verwertbarkeit, erfordern eine **selbstbestimmte und ausdrückliche Einwilligung** in die Nutzung der Daten und eine realistische Entscheidungsalternative zur Angabe der Daten. Soweit für den Bereich der wirtschaftlichen Verwertung die Daten als Entgeltsersatz eingesetzt werden, begibt sich der Dateninhaber in ein Austauschverhältnis, auf das die **allgemeinen Regeln für Schuldverhältnisse** anzuwenden sind. Der Widerruf der Einwilligung zur Nutzung von Daten ist hierbei an die allgemeinen Regeln zur Beendigung von Verträgen je nach Rechtsnatur durch Kündigung, Aufhebung, Widerruf oder Rücktritt vom Vertrag gebunden. Hierbei sind Ansprüche auf Schadensersatz der Gegenseite denkbar. Zum anderen muss eine Beendigung von langlaufenden Verträgen, d. h. die Lösung aus einem Dauerschuldverhältnis gem. § 314 BGB, immer möglich sein. Das Beispiel Amazon Underground zeigt, wie komplex eine Rückabwicklung sein kann.<sup>146</sup>

### **Verbraucherschutz als Lösung der Informationsasymmetrien**

*Herstellung von Privatautonomie und Durchsetzung von Verbraucherrechten heißt nicht Verhinderung von innovativen Geschäftsmodellen durch Verbot der Nutzung von Daten. Mehr Kommerzialisierung durch Unternehmen erfordert aber mehr individuelle Kontrolle*



*und Information der Verbraucher durch den Ausgleich von Informationsasymmetrien. Hierzu sollten standardisierte Einwilligungserklärungen für bestimmte Geschäftsmodelle und One-Pager erprobt werden.*

Bei der Nutzung von Big Data können eine Vielzahl von Daten beteiligter und unbeteiligter Personen erhoben werden, die hierauf keinen Einfluss haben. Insbesondere Verbraucher haben oft keinerlei Einflussmöglichkeiten, die Datenerhebung und -verarbeitung zu verhindern, da die Datenerhebung für sie oftmals im Verborgenen, d. h. ohne die Kenntnis der Betroffenen, geschieht oder weil es äußerst schwierig bis unmöglich ist, sich einer Überwachung zu entziehen. Verbraucherschutz im Wettbewerbsrecht soll bei unübersichtlichen Angeboten einen Überblick und bei komplexen Marktbedingungen Durchblick schaffen.<sup>147</sup>

*„Datenschutz war schon immer verbraucherrelevant.“<sup>148</sup> „Es gab noch nie eine Zeit, in der Daten so sehr der Gegenstand von Geschäftsmodellen geworden sind, deshalb wird Datenschutzrecht immer stärker Verbraucherschutzrecht werden.“<sup>149</sup>*

Nach dem Grünbuch soll für die Zulässigkeit der Datennutzung **der vom Unternehmen kommunizierte Zweck** im Mittelpunkt stehen.<sup>150</sup> Hierzu ist eine Diskussion der **Hierarchie der Nutzungszwecke** erforderlich. Die Erhebung und Verarbeitung von Big Data auf digitalen Plattformen können zum einen öffentlichen Interessen dienen, z. B. im Katastrophenschutz.<sup>151</sup> Gleichzeitig zielen die Anwendungen im zivilen Bereich überwiegend auf gewerbliche oder sonstige private Interessen. Diese unterschiedlichen Interessenlagen sind mit dem Recht auf informationelle Selbstbestimmung, dem Recht am eigenen Bild und vielen anderen Rechten in Einklang zu bringen. Die im Grünbuch geforderte „Transparenz und Information“ von Kunden sollte insbesondere bei Verbrauchern daran gemessen werden, wie viele Informationen erforderlich sind, damit die Souveränität und Kontrolle über die eigenen Daten gewahrt und die Entscheidungsfreiheit im

Marktgeschehen nicht unlauter beeinträchtigt wird. Bei einer Hierarchisierung der Nutzungszwecke kann **mehr Kommerzialisierung mehr individuelle Kontrolle und Information** erfordern. Diese Restriktion dient der Aufrechterhaltung eines fairen Leistungswettbewerbs. Nicht Verbot der Nutzung ist dann das Ziel, sondern Herstellung von Privatautonomie bei der Nutzung und Schutz des Verbrauchers bei einer Informations- und Kontrollinadäquanz. Unternehmen dürfen dann mehr kommerzialisieren, d. h. mehr Daten für unternehmerische Zwecke einsetzen, wenn sie dem Kunden mehr Transparenz und Kontrolle über seine Daten und deren Verwendung einräumen.

Neben einer Hierarchisierung der Nutzungszwecke bietet sich als Wertungsmaßstab auch die **Klassifizierung von Nutzungssphären** an. Leitlinie des Identity-Managements kann eine gestufte Einwilligung nach betroffenen Sphären sein. Die bisherigen Abgrenzungen des Öffentlichkeitsbegriffs, z. B. für Leistungsschutzrechte, taugen hierfür nur teilweise. Danach wird keine Öffentlichkeit hergestellt, wenn ein geschlossener, überschaubarer Nutzerkreis bzw. eine persönliche Verbundenheit besteht.<sup>152</sup> Soziale Netzwerke wie Facebook basieren zwar im Prinzip auf der Geschlossenheit der Nutzergruppe und dem Erfordernis der Anmeldung. Überschaubar ist die Zahl der Nutzer im Rechtssinne aber schon lange nicht mehr. Ein taugliches Abgrenzungskriterium in Bezug auf Transparenz und Kontrolle sind jedoch die **freiwillige Anmeldung zu einem Dienst** und die **aktive Zustimmung zu Nutzungsbedingungen**, unabhängig von der Problematik der Durchsetzung bereits geltenden Rechts.<sup>153</sup>

#### **Klarheit und Wahrheit im Wettbewerb**

*Das UWG bietet bei konsequenter Anwendung ausreichende Regelungen zum Schutz vor Irreführung im Wettbewerb bei digitalen Geschäftsmodellen.*

Durch das UWG sollen Wettbewerber, sonstige Marktteilnehmer, Verbraucher und der Wettbewerb an sich

nach den Maßstäben eines fairen Leistungswettbewerbs geschützt werden.<sup>154</sup> Das Gebot der Klarheit und Wahrheit von Werbung, die Transparenz der angebotenen Waren und Dienstleistungen und der Schutz des Verbrauchers vor einem Informationsungleichgewicht sind grundlegende Prinzipien des Wettbewerbsrechts. Regelungen zur Verwendung von Daten finden sich u. a. hinsichtlich der Zulässigkeit von Werbung im Direktmarketing<sup>155</sup>, des Anbietens von Diensten im Internet<sup>156</sup> und der Transparenz von Preisen<sup>157</sup>. Diese Regelungen sind auch Maßstab für neue Formen von Werbung und Datennutzung sowie -analyse bei digitalen Geschäftsmodellen.

So muss sich das Tracking von Nutzerverhalten zur Feststellung der individuellen Preisbereitschaft und zum **Anbieten von individuellen Preisen** an den Prinzipien der Klarheit und Wahrheit der Preise und der Preisfindung sowie der Offenlegung der diesbezüglichen Kriterien messen lassen. Soweit der Nutzer in die Verwendung seiner Daten einwilligt, ist die Datenanalyse nicht per se unzulässig, sondern genügt den Anforderungen des UWG, wenn die Kriterien der Preisfindung für den Nutzer offengelegt werden und so eine Irreführung ausgeschlossen werden kann.<sup>158</sup> Die zweite Grenze könnte die Schutzbedürftigkeit bestimmter Nutzergruppen wie z. B. geschäftlich unerfahrene Kunden, Kinder und Jugendliche sowie Menschen in Zwangssituationen sein, und die bewusste Ausnutzung dieser Situationen, siehe § 4a Abs. 1, Abs. 2 S. 1 Nr. 3 und S. 2 UWG. Diese Zwangssituationen sind bei Massentracking in der Regel kaum feststellbar. Ein Verstoß wird daher eher an der konkreten Handlung, der Art der beworbenen Produkte und Dienstleistungen sowie der sonstigen Kriterien des § 4a Abs. 2 UWG festzumachen sein.

Für das Anbieten von Diensten über **Plattformen** ist die Herstellung von Transparenz hinsichtlich Rolle, Produkten und Dienstleistungen, Preisen und Bedin-

gungen erforderlich. Bezüglich der Rolle ist zunächst festzustellen, ob eigene oder fremde Dienste angeboten werden und ob auf das Angebot der Plattform überhaupt Einfluss genommen werden kann. Nur dann liegt ein Diensteanbieter vor.<sup>159</sup> Dann sollte eine Angabe in Bezug auf das Anbieten von eigenen Diensten oder das bloße Vermitteln gemacht werden. Ein ausdrücklicher Hinweis im Sinne einer **Mitteilung** ist bei gesetzlichen Mitteilungspflichten wie denen von Versicherungsmaklern erforderlich, siehe z. B. § 11 VersVmG. „Mitteilen“ ist nach dem LG München I mehr als „Bereithalten“ (unter einem Button „Erstinformation“), es bedeutet vielmehr aktives Präsentieren, ohne dass der Kunde danach suchen muss.<sup>160</sup> Für Dienste ohne besondere Mitteilungspflichten sehen §§ 5, 6 TMG allerdings nur ein **Bereithalten** der Informationen vor (leicht erkennbar, unmittelbar erreichbar und ständig verfügbar). Hierfür ist das Bereithalten unter einem Button „Impressum“ oder „Kontakt“ ausreichend.<sup>161</sup>

#### Impulse für den Rechtsrahmen 4.0

*Ob Recht 4.0 Innovationsmotor oder -hemmnis sein wird, hängt von der Kohärenz und Stringenz bei der Gestaltung der gesetzlichen Regelungen ab. Die folgenden Regelungen sind zur Konkretisierung der Rechtsrahmens für digitale Plattformen erforderlich:*

- Klarstellung des ökonomischen Wertes von Daten und des Charakters als Entgelt substituierende Gegenleistung in Austauschverhältnissen;
- bei Daten als Gegenleistung im Austauschverhältnis: Qualifizierung des Rückrufs der datenschutzrechtlichen Einwilligung als Kündigung, Rücktritt oder Widerruf des Vertragsschlusses;
- technische Konkretisierung der Verpflichtung zur Bereitstellung von Daten und Formaten;
- Ausnahmeregelungen für Start-ups und KMU bei der Erfüllung der technischen Standards mit den Anknüpfungskriterien Nutzerzahlen, Netzwerkeffekte etc.;

- Schutz der Investition in eine Datenbank durch Klarstellung der Trennung der Rechte an Daten von den Rechten des Datenbankherstellers;
- Verpflichtung der Kennzeichnung der Anbieter von Plattformen als Anbieter, Vermittler von Diensten oder Aufbereiter von Informationen;
- Zulässigkeit neuer Geschäftsmodelle ohne diskriminierende Kennzeichnungen, aber mit konsequenter Anwendung der Kriterien der Irreführung des UWG durch
  - Klarstellung der Zulässigkeit individueller Preise,
  - unter Beachtung der Kriterien des § 19 AGG und Grenze des § 4a UWG bei besonders schutzbedürftigen Kundengruppen sowie Verpflichtung zur
  - Information über Preisbestandteile und-kriterien,
    - Informationen über Quellen und dem Algorithmus zugrunde liegende Wertungs- und Ordnungskriterien bei der Aufbereitung von Informationen,
    - Information über Provisionen für die Platzierung bei Suchmaschinen oder Vergleichsportalen;
- konsequente Anwendung des Prinzips der Trennung von redaktionellem Inhalt und Werbung;
- Experimentierklauseln für bestimmte digitale Plattformen
  - zur Nutzung von Big Data aus verschiedenen Quellen und/oder
  - zu sich verändernden Zwecken,
  - bei Einsatz von standardisierten, übersichtlichen und transparenten Einwilligungserklärungen zum Ausgleich der Informationsasymmetrie und zur Kompensation der besonderen Einsatzrisiken, bei deren Einsatz sich der Nutzer auf bestimmte rechtliche Qualitätskriterien verlassen kann;
- standardisierte Einwilligungserklärungen für bestimmte Geschäftsmodelle durch Gesetz oder Branchenvereinbarung (vergleichbar der Widerrufserklärung im Fernabsatz), ggf. verbunden mit Zertifizierungsmodellen;
- Vorstellen eines One-Pagers<sup>162</sup> vor jede ausführliche Information zum Datenschutz.



- <sup>110</sup> Zum fehlenden Maßstab etwa Kuner, Cate, Millard, Svantesson, Lynskey, Editorial – Risk management in data protection, *International Data Privacy Law*, 2015, Vol. 5, No. 2; zu den aufmerksamkeitsökonomischen Gesichtspunkten v. a. Hallinan and Friedewald, *Public Perception of the Data Environment and Information Transactions – A selected-survey analysis of the European public’s views on the data environment and data transactions*, S. 72–74.
- <sup>111</sup> Siehe etwa die Ofcom-Studie „Personal Data and Privacy“ zur Einwilligung, zuletzt heruntergeladen am 01.08.2016 unter [http://www.wik.org/fileadmin/Studien/2015/Personal\\_Data\\_and\\_Privacy.pdf](http://www.wik.org/fileadmin/Studien/2015/Personal_Data_and_Privacy.pdf).
- <sup>112</sup> Zum Schutzbereich siehe Grafenstein DuD 2015, 789 (791).
- <sup>113</sup> Grafenstein und Schulz, a. a. O., S. 264/265.
- <sup>114</sup> Vgl. Britz, a. a. O., S. 274 ff.
- <sup>115</sup> Siehe zur Anforderung aus Artikel 6 Abs. 1 b) der Datenschutzrichtlinie 95/46/EC, die Zwecke „eindeutig“ festzulegen (bzw. nach der englischen Fassung „explizit“ zu machen), Artikel-29-Datenschutzgruppe, opinion 03/2013 on purpose limitation, S. 17 ff.
- <sup>116</sup> So auch Art. 13 Abs. 3 und Art. 14 Abs. 4 der DSGVO (EU) 2016/679.
- <sup>117</sup> Vgl. Albers, a. a. O., Rn. 124, siehe etwa auch Däubler/Klebe/Welde/Weichert, BDSG, § 4a Rn. 18.
- <sup>118</sup> Vgl. zur höheren Rechtsunsicherheit beim Einsatz rechtlicher Prinzipien allgemein etwa Eifert, Regulierungsstrategien, in: Hoffmann-Riem, Schmidt-Aßmann, Voßkuhle (Hrsg.), *Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation“*, 2012, Rn. 25 und 26; Franzius, Claudio, Modalitäten und Wirkungsfaktoren der Steuerung durch Recht, in: Hoffmann-Riem, Schmidt-Aßmann, Voßkuhle (Hrsg.), *Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation“*, 2012, Rn. 7, 17 und 81–103.
- <sup>119</sup> Instruktiv Eifert, a. a. O., Rn. 52 ff.; jetzt auch umfassend vorgesehen in den Artikeln 40–43 der DSGVO (EU) 2016/679.
- <sup>120</sup> Vgl. u. a. Art. 24 Abs. 3 der DSGVO (EU) 2016/679.
- <sup>121</sup> Vgl. Art. 46 Abs. 2 f) der DSGVO (EU) 2016/679.
- <sup>122</sup> Grünbuch, S. 56.
- <sup>123</sup> Grünbuch, S. 34.
- <sup>124</sup> Grünbuch, S. 32, 58.
- <sup>125</sup> Grünbuch, S. 15, 57, 60.
- <sup>126</sup> Grünbuch, S. 34.
- <sup>127</sup> Entwurf eines Neunten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen (9. GWB-ÄndG), Referentenentwurf, Bearbeitungsstand: 01.07.2016, S. 36 f., 40.
- <sup>128</sup> Entwurf RiLi COM(2015) 634 final der EU-Kommission vom 09.12.2015; Grünbuch S. 32, 58.
- <sup>129</sup> Referentenentwurf, Begründung S. 48.



- <sup>130</sup> Kritik der Monopolkommission, Hauptgutachten XXI, Wettbewerb 2016 vom 20.09.2016, S. 11.
- <sup>131</sup> Haucap, Justus: Ordnungspolitik und Kartellrecht im Zeitalter der Digitalisierung, in: Ordnungspolitische Perspektiven Nr. 77, S. 13.
- <sup>132</sup> Art. 3 Abs. 1 VO 330/2010, Art. 5 VO 461/2010 (Kfz-GVO), Kfz-Leitlinien Nr. 62–64.
- <sup>133</sup> § 20a Abs. 3 EnWG, § 20 StromGKV und GasGKV.
- <sup>134</sup> § 46 TKG.
- <sup>135</sup> Monopolkommission: Hauptgutachten XXI, Wettbewerb 2016 vom 20.09.2016, S. 11.
- <sup>136</sup> Art. 20 DSGVO: Nach ErwGr (68) sollen interoperable Formate entwickelt werden.
- <sup>137</sup> Referentenentwurf, Begründung S. 75 f.; die Monopolkommission hatte sogar einen Transaktionswert von 500 Mio. Euro empfohlen: Sondergutachten 68, Wettbewerbspolitik: Herausforderung digitale Märkte vom 01.06.2015, Tz. 461.
- <sup>138</sup> Deutscher Bundestag, Wissenschaftlicher Dienst, Horvath, Sabine: Big Data, Nr. 37/13 vom 06.11.2013, S. 1; Handelsblatt Research Institute: Big Data und Datenschutz, Studie erstellt für die Deutsche Telekom, S. 3, 10/2013.
- <sup>139</sup> Zusammengesetzt aus Dataprotection und Sustainability, siehe CeBIT 2014, [www.cebit.de/de/news-trends/trends/datability/](http://www.cebit.de/de/news-trends/trends/datability/), Stand: 31.03.2014.
- <sup>140</sup> § 3a BDSG: Datenvermeidung, Art. 25 Abs. 1 DSGVO: Datenminimierung.
- <sup>141</sup> RiLi COM(2015) 634 final der EU-Kommission vom 09.12.2015.
- <sup>142</sup> Siehe hierzu: Duisberg, Alexander: „Datenhoheit und Recht des Datenbankherstellers – Recht am Einzeldatum vs. Recht an Datensammlungen“, wird demnächst veröffentlicht.
- <sup>143</sup> Picot, Arnold: „Recht auf Ökonomisierung der eigenen Daten – Privatheit, Freiheit und Reversibilität“, Vortrag beim Workshop Begleitforschung Recht zu „Innovations from Smart Data“ am 08.09.2016, [www.gi.de/smart-data-begleitforschung/workshops-2016/3-workshop-der-fg-recht.html](http://www.gi.de/smart-data-begleitforschung/workshops-2016/3-workshop-der-fg-recht.html).
- <sup>144</sup> EuGH-Urteil vom 13.05.2014, Rs C-131/12 und Art. 17 DSGVO.
- <sup>145</sup> Art. 20, 21 DSGVO.
- <sup>146</sup> [www.amazon.de/Amazon-com-Amazon-Underground/dp/B004GJDQT8](http://www.amazon.de/Amazon-com-Amazon-Underground/dp/B004GJDQT8), Stand: 30.09.2016.
- <sup>147</sup> Leitbild der Bundesverbraucherzentrale, abrufbar unter: [www.verbraucherzentrale.de/wir-ueberuns](http://www.verbraucherzentrale.de/wir-ueberuns), Stand: 09.10.2015.
- <sup>148</sup> Dr. Thilo Weichert, „Datenschutzrecht für den Verbraucher“, Vortrag auf der Computas-Fachkonferenz DuD 2001 am 23. und 24.04.2001 in Berlin.
- <sup>149</sup> Heiko Maas: Für den Datenschutz in der digitalen Gesellschaft – Modernes Recht aus Brüssel und Berlin!, Vortrag beim 16. Datenschutzkongress, 06.05.2015, Berlin; [www.bmjv.de/SharedDocs/Reden/DE/2015/20150506\\_Datenschutzkongress.html](http://www.bmjv.de/SharedDocs/Reden/DE/2015/20150506_Datenschutzkongress.html).
- <sup>150</sup> Grünbuch, S. 57.

- <sup>151</sup> Siehe Programm des BMWi „Innovations from Smart Data“, Projekt sd-kama.
- <sup>152</sup> § 15 Abs. 3 UrhR, Ahlberg/Götting, in: UrhR, BeckOK, Stand: 01.07.2016, Rdn. 25.
- <sup>153</sup> Siehe den oben geschilderten Stand zu WhatsApp/Facebook.
- <sup>154</sup> § 1 und § 3 UWG.
- <sup>155</sup> § 7 Abs. 2 und 3 UWG.
- <sup>156</sup> Telemedien: §§ 5, 6, 11 f. und 13 ff. TMG.
- <sup>157</sup> § 1 ff. PAnGVO, § 3 Abs. 1 i. V. m. § 5 Abs. 1 UWG.
- <sup>158</sup> § 3 Abs. 1 i. V. m. § 5 Abs. 1 Nr. 2 bzw. § 5a Abs. 2 und 3 Nr. 3 UWG.
- <sup>159</sup> LG Heidelberg, Urteil vom 30.12.2015, Az 12 O 21/15, BeckRS 2016/04060.
- <sup>160</sup> LG München I, Urteil vom 13.07.2016, Az 37 O 152 68/15 für Versicherungsmakler mit Verpflichtung aus § 11 VersVmG.
- <sup>161</sup> BGH-Urteil vom 20.07.2006, MMR 2007, 40 f., noch für TDG: Erreichbarkeit über zwei Klicks.
- <sup>162</sup> [www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2015/11192915\\_Vorstellung\\_OnePager.html](http://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2015/11192915_Vorstellung_OnePager.html).
- <sup>163</sup> Vgl. BDSG § 3 (7).
- <sup>164</sup> Vgl. Abschnitt 1.
- <sup>165</sup> Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad; Security Patterns: Integrating Security and Systems Engineering
- <sup>166</sup> A. Pretschner, M. Hilty, D. Basin, C. Schaefer, T. Walter; Mechanisms for Usage Control.
- <sup>167</sup> George Coker, Joshua Guttman, Peter Loscocco, Amy Herzog, Jonathan Millen, Brian O’Hanlon, John Ramsdell, Ariel Segall, Justin Sheehy, and Brian Sniffen; Principles of Remote Attestation.
- <sup>168</sup> <http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/>.
- <sup>169</sup> Förderkennzeichen: 01IC12S01F (BMBF).
- <sup>170</sup> SECCRIT, <http://www.seccrit.eu>, grant agreement no 312758.
- <sup>171</sup> Usage Control, Fraunhofer IESE, <http://s.fhg.de/UC>.
- <sup>172</sup> Projekt NGCert, Förderkennzeichen: 16KIS0078 (BMBF).
- <sup>173</sup> Art. 42 f. DSGVO sehen die Möglichkeit vor, mittels Zertifizierung die Einhaltung der Datenschutzvorgaben nachzuweisen. Die Zertifizierung kann sich grundsätzlich auf sämtliche datenschutzrechtlich relevanten Verarbeitungsvorgänge beziehen. So sind, wie in diesem Dokument angeregt, auch die Standardisierung und Zertifizierung von Verarbeitungszwecken denkbar, siehe Grafenstein, S. 27.
- <sup>174</sup> Vgl. <https://specifications.xbrl.org/work-product-index-group-base-spec-base-spec.html>
- <sup>175</sup> Vgl. <http://www.edgar-online.com/>.



# Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data

---

Datenschutzgrundprinzipien im Diskurs

# Impressum

## Herausgeber

Smart-Data-Begleitforschung  
FZI Forschungszentrum Informatik  
Außenstelle Berlin  
Friedrichstr. 60, 10117 Berlin  
[www.smart-data-programm.de](http://www.smart-data-programm.de)

## Konzeption und Gestaltung

LoeschHundLiepold Kommunikation GmbH, Berlin

## Stand

November 2016

## Druck

NN

## Bildnachweis

Sergey Nivens – Fotolia.com (Titel)

Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Energie

aufgrund eines Beschlusses  
des Deutschen Bundestages