Institut für Zivilrecht

Univ.-Prof. Dr. Christiane Wendehorst, LL.M.
Schottenbastei 10-16 (Juridicum)
A-1010 Wien

T +43-1-4277-34820
F +43-1-4277-834820
christiane.wendehorst@univie.ac.at
http://zivilrecht.univie.ac.at/wendehorst

An den

Ausschuss für Konsumentenschutz

Wien, am 02.05.2019

Stellungnahme zu den Anträgen

102/A(E) betreffend Allgegenwärtige Überwachung im Internet der Dinge auf Kosten des Konsumentenschutzes

105/A(E) betreffend Allgegenwärtige Überwachung im Internet der Dinge auf Kosten des Konsumentenschutzes - insbesondere der Smart-Cars

GZ. 13655.0060/1-L1.3/2019

Eine intensive Beschäftigung des österreichischen Gesetzgebers mit den Problemen des digitalen Konsumentenschutzes ist **überfällig**, und die beiden Entschließungsanträge sind **insofern uneingeschränkt zu unterstützen**.

Beispiele: (1) Bei Inbetriebnahme eines smarten Fernsehers erklärt sich der Nutzer damit einverstanden, dass sein Fernsehverhalten und im Wohnzimmer gesprochene Worte ausgewertet und für personalisierte Werbung, einschließlich personalisierter Wahlwerbung, genutzt werden. (2) Die mit Hilfe eines Smart-Car erhobenen Mobilitätsdaten werden dazu genutzt, besondere Bedarfslagen zu erkennen und für personalisierte Preisbildung auszuwerten (3) Eine Reparatur der ‚smarten' Bewässerungsanlage im Garten verlangt Zugriff auf in der Cloud gespeicherte Daten, aber der Hersteller gewährt den Zugang nur teuren Vertragswerkstätten. (4) Der Hersteller der intelligenten Heizungsanlage verlangt beim Weiterverkauf der Immobilie eine höhere Summe, um ein Nutzerkonto für den neuen Eigentümer anzulegen. (5) Der Anbieter eines vernetzten Fitness-Armbands liefert bei einem Anbieterwechsel zwar Rohdaten, aber nicht Trainingspläne und Statistiken. (6) Der Leasingnehmer eines Smart-Cars erklärt sich damit einverstanden, dass das Smart-Car bei Verzug mit Leasingraten ohne Vorwarnung automatisch gesperrt wird.

Die Unterfertigte ist seit Jahren bemüht, Bewusstsein für die Thematik zu wecken und die Entwicklung voranzutreiben. Sie ist in diesem Zusammenhang u.a. für die Europäische Kommission, das Europäische Parlament, das European Law Institute und die deutsche Bundesregierung als Beraterin bzw. Gutachterin tätig geworden. Die während der österreichischen Ratspräsidentschaft erfolgreich verhandelte neue Warenhandelsrichtlinie entspricht insofern, als Waren mit digitalen Elementen und damit Probleme des IoT betroffen sind, weitgehend Regulierungsvorschlägen, welche die Unterfertigte in den Jahren 2016 bis 2018 veröffentlicht hat. Als Vorsitzende der zivilrechtlichen Abteilung des Österreichischen Juristentages (ÖJT) hat sie die Befassung des 20. ÖJT mit vertragsrechtlichen Problemen der Digitalisierung initiiert und wird als Gutachterin des 21. ÖJT zur Durchsetzung von Konsumentenrechten ganz wesentlich auf digitale Entwicklungen eingehen. Sie ist derzeit auch Co-Sprecherin der Datenethikkommission der deutschen Bundesregierung (DEK), betont aber, diese Stellungnahme allein im eigenen Namen abzugeben.

Zu den **Problemen des IoT für KonsumentInnen** und möglichen **Bausteinen eines digitalen Konsumentenschutzes** in Österreich sei ohne jeden Anspruch auf Vollständigkeit – und beschränkt auf wenige speziell zivilrechtliche Beispiele – kurz Stellung genommen:

1. Besserer Schutz durch datenspezifisches Vertrags- und Haftungsrecht

Das IoT birgt für KonsumentInnen in erster Linie Gefahren in Bezug auf den Datenschutz. Diesbezüglich ist nationale Gesetzgebung aufgrund der Sperrwirkung der Datenschutz-Grundverordnung (DSGVO) allerdings nur noch möglich, soweit

a. eine Öffnungsklausel der DSGVO nationale Gesetze zulässt (z.B. in Bezug auf Gesundheitsdaten)
b. Maßnahmen nicht rechtlicher Art sind (z.B. Forschung zu datenschutzfreundlichen Technologien)
c. Maßnahmen außerhalb des Anwendungsbereichs der DSGVO liegen (z.B. anonymisierte Daten)
d. gesetzgeberische Maßnahmen andere als von der DSGVO geregelte Fragen betreffen.

Besonderes Augenmerk ist nach Auffassung der Unterfertigten auf Punkt d. zu werfen. Die DSGVO stellt eine große Errungenschaft dar, aber es dürfen die Erwartungen an diesen Rechtsakt nicht überspannt werden. Wenn andere als vom Regelungszweck der DSGVO umfasste Pflichten verletzt werden, muss es auch jenseits der DSGVO zu Schadenersatzansprüchen kommen, etwa wegen **Verletzung vertraglicher Schutz- und Treuepflichten** oder auch nach **Deliktsrecht**.

Zu den Säulen des Datenschutzrechts gehört die Einwilligung des Betroffenen. Allerdings ist der Rechtsordnung eine Freiheit zur beliebigen Selbst- oder Fremdschädigung nicht bekannt. Vielmehr sind hier von der DSGVO gar nicht berührte materielle Schranken anzuerkennen, die beispielsweise in der **Inhaltskontrolle von AGB** (vgl. DSGVO Erwägungsgrund 42) oder in der Unwirksamkeit aus Gründen der **Sittenwidrigkeit** zum Ausdruck kommen können.

Nach Auffassung der Unterfertigten besteht hier besonderes Potenzial für einen **österreichischen digitalen Konsumentenschutz**. Maßnahmen würden sich zwar stets in einer europarechtlichen Grauzone bewegen, und es bestünde stets die Gefahr, dass der EuGH die DSGVO für abschließend erklärt. Die Unterfertigte empfiehlt allerdings, hier **mutig voranzuschreiten** und nicht aus Furcht vor einer allfälligen negativen Entscheidung des EuGH von Vornherein untätig zu bleiben.

2. Kein Bedarf nach „Dateneigentum“

Von der Einführung von „Dateneigentum“ im Sinne eines Ausschließlichkeitsrechts, das Ähnlichkeit entweder mit dem Sacheigentum oder aber mit geistigem Eigentum (z.B. Verwertungsrechte ähnlich wie beim Urheberrecht) hätte, wird **ausdrücklich abgeraten**. Das betrifft auch Daten aus Smart-Cars.

Dem Einzelnen stehen bereits jetzt aufgrund des Datenschutzrechts oder des allgemeinen Zivilrechts genügend Rechtspositionen mit Drittwirkung zu, deren Einschränkung er theoretisch nur gegen Zahlung eines entsprechenden Entgelts dulden müsste. So könnte der Einzelne etwa theoretisch schon seine datenschutzrechtliche Einwilligung oder die Nutzung seines SmartCars für Zwecke der Datenwirtschaft von jeder beliebigen geforderten Gegenleistung abhängig machen – aber eben nur theoretisch. Praktisch gelingt ihm ein solcher Verhandlungserfolg nicht, und zwar aufgrund von Umständen, die nichts mit dem Fehlen eines weiteren eigentumsähnlichen Verwertungsrechts zu tun haben. Hätte er ein solches weiteres Recht, würde er es ebenso **vertraglich aufgeben** wie er seine derzeit bestehenden Rechtspositionen vertraglich aufgibt.

Die Asymmetrie der Verhandlungsposition ließe sich theoretisch durch die Einführung von Verwertungsgesellschaften (ähnlich etwa der Litera.mechana) ändern. Eine wirtschaftliche Komponente personenbezogener Daten in Anlehnung an die Verwertungsrechte beim Urheberrecht stünde allerdings in einem potenziellen **Spannungsverhältnis zum Datenschutz**, insbesondere zur Freiwilligkeit und jederzeitigen Widerruflichkeit der Einwilligung und zum Löschungsanspruch. Das Wesen von urheberrechtlichen Verwertungsrechten ist es ja gerade, dass ich sie unwiderruflich einem Anderen einräumen kann.

Zudem würden durch die Einführung derartiger Vergütungsmodelle **zweifelhafte finanzielle Anreize** zur Produktion möglichst vieler personenbezogener Daten geschaffen und würden gerade besonders vulnerable Personen (z.B. Minderjährige, einkommensschwache Bevölkerungsgruppen) zur Preisgabe möglichst vieler Daten animiert. Eine Einpreisung der Vergütungen würde zudem zu einer verhältnismäßigen Mehrbelastung

datenschutzbewusster Personen führen.

Die genannten Argumente gegen Dateneigentum gelten zwar nicht in gleichem Maße in Bezug auf anonymisierte Daten. Angesichts der Vielzahl von Akteuren, die einen Beitrag zur Generierung und Veredelung von Daten leisten, würde ein faires Vergütungssystem allerdings ein Maß an Komplexität erreichen und ein Ausmaß an **Allzeitüberwachung** zwecks Messung von Datenflüssen erfordern, das außer Verhältnis zu jedem möglichen Gerechtigkeitsgewinn stünde.

3. Schlüsselrolle der vertraglichen Inhaltskontrolle

Nach Auffassung der Unterfertigten ist das Klausel-Recht, das derzeit v.a. in § 6 KSchG sowie in §§ 864a, 879 ABGB geregelt ist, geradezu der **optimale Ansatzpunkt für einen österreichischen digitalen Konsumentenschutz**, weil in Erwägungsgrund 42 DSGVO zumindest für die Einwilligung ausdrücklich auf die Klausel-RL Bezug genommen wird. Außerdem ist das Klauselrecht einer der wenigen Bereiche, der noch nicht auf EU-Ebene einer Vollharmonisierung unterzogen wurde, so dass hier viel nationale Gestaltungsfreiheit besteht. Dabei ist vorrangig an eine Nachschärfung der Klauselverbote in § 6 Abs 1 und 2 KSchG zu denken. Trotz der immensen wirtschaftlichen Bedeutung von Daten für KonsumentInnen fehlt es derzeit an **datenspezifischen Klauselverboten**.

Datenschutzrecht betrifft nur personenbezogene Daten und adressiert von seinem Schutzzweck her nicht die konkrete Ausgewogenheit vertraglicher Rechte und Pflichten. Daher bedarf es eines vertragsrechtlichen Schutzes insoweit, als entweder nicht-personenbezogene Daten betroffen sind (z.B. viele Gerätedaten, soweit sie einem Individuum nicht zugeordnet werden können) oder es um andere Interessen als das Persönlichkeitsrecht geht (z.B. Vermögensinteressen). Die Unterfertigte möchte beispielhaft Klauseln nennen betreffend die

- Verwehrung oder unangemessene Erschwerung des Zugangs zu Gerätedaten, die für die übliche Nutzung eines Geräts, einschließlich **Reparatur durch eine unabhängige Werkstätte**, erforderlich sind;
- Verwehrung oder unangemessene Erschwerung eines betriebsnotwendigen Datenzugangs für den **Zweiterwerber** einer vernetzten Sache (z.B. bei Verkauf einer mit Smart Home Equipment ausgestalteten Immobilie);
- sonstige datenbezogene Erschwerung des **Weiterverkaufs oder der Weitervermietung** vernetzter Sachen oder ihrer Nutzung als Kreditsicherheit (z.B. durch Gewährung vollen Zugriffs auf sensible Daten für den Zweiterwerber);
- Erschwerung des **Anbieterwechsels** durch Lock-in veredelter Daten wie z.B. Datenanalysen, für die der Nutzer wirtschaftlich betrachtet bereits bezahlt hat;
- vertragliche Vereinbarung der **ferngesteuerten Stilllegung** von Geräten (z.B. Smart-Cars) durch Sperre von Nutzerkonten oÄ, etwa zum Zweck der Forderungsbetreibung.

4. Gewährleistungsähnliche Herstellerhaftung

Zum Schutz der KonsumentInnen muss das Haftungsrecht der Entwicklung gerecht werden, wonach die Nutzbarkeit von auch hochwertigen Gütern (Immobilien, Maschinen, Kraftfahrzeuge usw.), die bei KonsumentInnen oft nahezu das gesamte Vermögen ausmachen, immer mehr von der **langfristigen Erbringung digitaler Dienste** abhängig ist (Software-Updates, Nutzerkonten u.a.). Nach derzeit geltendem Recht ist weder die langfristige Erbringung der Dienste an sich noch deren Erbringung bei Weitervermietung oder Weiterverkauf vernetzter Gegenstände gesichert. Allerdings schließt der Nutzer nach wie vor Kaufverträge ab und tritt gegenüber einem Händler mit einer Summe in Vorleistung, die den Wert der gesamten erwarteten Nutzungsdauer widerspiegelt.

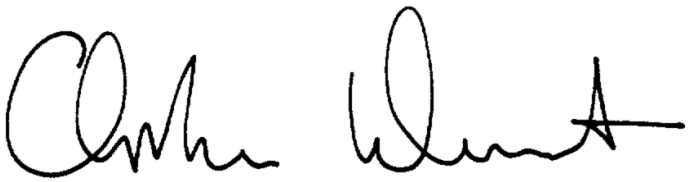
Die neue **Richtlinie zum Warenhandelskauf** ist hier bereits einen großen Schritt in die richtige Richtung gegangen, bürdet aber die gesamte Verantwortlichkeit dem Händler auf und erfasst auch nicht alle Situationen (z.B. nicht den praktisch besonders wichtigen Kauf einer Immobilie mit vernetzten Komponenten). Der Händler ist allerdings nicht derjenige Akteur, der entstehende Kosten am leichtesten vermeiden bzw. die betreffenden Risiken am ehesten kontrollieren kann, und bei nicht unternehmerisch handelnden Verkäufern verbietet sich deren Belastung mit dem Risiko künftiger Updates etc. von Vornherein. Die Unterfertigte empfiehlt daher die Hersteller von Komponenten und Anlagen auch insoweit in die Pflicht zu nehmen („**gewährleistungsähnliche Herstellerhaftung**"). Dies hätte zusätzlich den Vorteil, dass Konstellationen, wie wir sie derzeit beim **„Diesel-Skandal"** erleben, einer für die KonsumentInnen angemessenen und eindeutigen Lösung zugeführt werden könnten.

5. Deliktische Produzentenhaftung und Vertrag mit Schutzwirkung zugunsten Dritter

Zum Schutz der österreichischen KonsumentInnen bedarf es einer raschen **Standardisierung** von Anforderungen an die **digitale Produktsicherheit** und eine entsprechende Überarbeitung der Rechtslage auf europäischer Ebene, wobei notfalls auch verbleibende nationale Kompetenzen umfassend zu nutzen wären. Produktsicherheit muss dabei **IT-Sicherheit** (Schutz vor Verletzungen der Privatsphäre, vor missbräuchlichem Ausspähen für Zwecke von Einbruchsdiebstählen, vor Fremdsteuerung der Geräte, usw.) und **Datenschutz** umfassen, namentlich Privacy by Design und Privacy by Default. Diese Anforderungen müssen nicht nur erfüllt sein, wenn ein Produkt ausgeliefert wird, sondern dürfen auch bei späteren Software-Updates nicht verloren gehen; umgekehrt sollte den Hersteller bei später auftretenden Sicherheitslücken – entsprechend den Regelungen in den Richtlinien zu digitalen Inhalten und digitalen Dienstleistungen sowie zum Warenhandel – im Rahmen der berechtigten Konsumentenerwartungen eine Pflicht zu Sicherheitsupdates treffen. Insgesamt kommt der laufenden **Produktbeobachtung** und **Produktpflege** eine gesteigerte Bedeutung zu.

Aufgrund der Vollharmonisierung der Produkthaftung durch die Produkthaftungs-RL, die zwar derzeit einer Überprüfung unterzogen wird, gegen deren Änderung auf europäischer Ebene aber massive Lobby-Arbeit betrieben wird, sind nationale Maßnahmen im Bereich des PHG nicht möglich. Der österreichische Gesetzgeber bzw die österreichischen Gerichte haben aber weiterhin erhebliche Spielräume, was das **nationale Deliktsrecht des ABGB und den Vertrag mit Schutzwirkung zugunsten Dritter** betrifft. Die Unterfertigte empfiehlt, diese nationalen Spielräume umfassend auszuschöpfen.

Die vorgenannten Punkte sollen nur als wenige Beispiele aus den zivilrechtlichen Forschungsgebieten der Unterfertigten verstanden werden, wo ein österreichischer digitaler Konsumentenschutz ansetzen könnte.



Univ.-Prof. Dr. Christiane Wendehorst, LL.M.