SVRV Sachverständigenrat für Verbraucherfragen

Verbraucherpolitik in der digitalen Welt:
Standpunkte des Sachverständigenrates für Verbraucherfragen

Übergeordnetes Ziel einer verbraucherbezogenen Netzpolitik sollte sein, die digitale Welt verbraucherfreundlicher zu gestalten, so dass gerechtfertigtes Vertrauen in die digitalen Angebote entstehen kann, die digitalen Märkte attraktiv werden und ihre Vorteile möglichst vielen Verbraucherinnen und Verbrauchern zugutekommen.

1. Bereitstellung qualitativ hochwertiger, einfacher, verständlicher und überprüfbarer Informationen und Behebung von Informations-, Gestaltungs- und Betroffenheitsungleichgewichten

Empfehlungen:

- Datenschutzerklärungen und Allgemeine Geschäftsbedingungen (AGB) sollten hinsichtlich Umfang, Lesbarkeit, Verständlichkeit und Deutlichkeit sowie Länge des Textes vereinfacht bzw. – an Verbraucherkompetenzen angepasst – „übersetzt“ werden (z. B. bildliche Darstellung durch Icons).
- Die Verwender von AGB sollten verpflichtet werden, die Kernaussagen auf einem einseitigen Informationsblatt zusammenzufassen.
- Eine Software zur rechtlichen Überprüfung der zum Teil Hunderte von Seiten langen AGB ist zu entwickeln. Die Möglichkeiten einer digitalisierten schematischen Kontrolle sind gegeben und müssen nur weiter entwickelt werden.
- Seitens des Gesetzgebers sollten konkrete standardisierte Muster zur Produktinformation vorgegeben werden, die digital leicht verfügbar sind und von denen grundsätzlich nicht abgewichen werden darf.
- Der Einsatz standardisierter Produktinformation ist sehr eng mit dem möglichen Nutzen der Digitalen Finanzberatung verknüpft:
- Alle Anbieter, unabhängig vom Zugangskanal oder Beratertyp sowie vom Unternehmenssitz, die in Deutschland eine Finanzdienstleistung verkaufen wollen, sollen verpflichtet sein, unabhängig vom Kaufzeitpunkt öffentlich zugänglich zu allen ihren Finanzdienstleistungen eine standardisierte Produktinformation bereitzustellen. Dann können potentielle Nutzer einfach, verständlich und vergleichbar beurteilen, welche Risiken bestehen, welche Kosten direkt und

indirekt bei der Nutzung entstehen und welche Serviceleistungen und Zahlungsdienste mit dem Zahlungskonto unmittelbar verbunden sind.

- Es wird die Einrichtung eines öffentlich finanzierten Instituts empfohlen, das klar verständliche und evidenzbasierte Informationen über Nutzen und Schaden aller wesentlichen
- Tests, Impfungen, Medikamente und Behandlungen im Netz und auf mHealth-Technologien (wie Smartphones) zur Verfügung stellt sowie hilft, existierende verlässliche Quellen zu finden.
- Nach englischem Vorbild wäre zu überlegen, den Verbraucherorganisationen die Möglichkeit einzuräumen, bei verbraucherschutzgesetzeswidrigen Praktiken ein Eingreifen der staatlichen Aufsicht zu erzwingen.

2. Bewusste und freiwillige Einwilligungen in Erhebung, Nutzung und Verwendung von Verbraucherdaten

Empfehlungen:

- Das Verständnis der Vertragsbedingungen bei den Verbraucherinnen und Verbrauchern ist durch Änderung der AGB zu stärken. Das kann nur durch Vereinfachung und Kürzung gelingen.
- Es muss Transparenz über die möglichen Konsequenzen von Einwilligungen bestehen.
- Für eine über die ursprünglich erteilte Einwilligung hinausgehende Nutzung von Verbraucherdaten sollte eine erneute ausdrückliche Einwilligung erforderlich ein.
- Zeitlich befristete Einwilligungen, die regelmäßig erneuert werden müssten, werden für sinnvoll erachtet.
- Aus den digitalen Angeboten muss für Bürgerinnen und Bürger klar und verständlich erkennbar sein, inwieweit und mit welchen persönlichen Daten bezahlt werden soll, auch durch die Weitergabe an Dritte. Außerdem müssen im Ablehnungsfall alternative Formen möglich sein (Wettbewerb), die Nicht-Nutzung einer Beratung genügt nicht.

3. Transparenz über die Verwertung personenbezogener Daten, über die den Algorithmen zugrunde liegenden Kriterien sowie über den Wert der eigenen Daten herstellen

Die Intransparenz der Datensammlung, -speicherung und -verwendung sowie der faktische Ausschluss vom Online Handel für diejenigen, die ihre Daten nicht oder nur teilweise preisgeben möchten, machen deutlich, dass die individuellen Sicherheitsinstrumente wie Zustimmung, Opt-out und Anonymisierung in der Big-Data-Welt nicht weit genug reichen. Der Staat muss ergänzend die Aufgabe übernehmen, grundsätzliche Sicherheit und den Schutz der Privatsphäre zu gewährleisten, damit Verbraucher keiner „Black Box“ der Datenanalyse und Datensammlung ausgesetzt sind.

Empfehlungen:

- Verbraucherinnen und Verbraucher müssen die Möglichkeit haben, aktiv über die Sammlung, Analyse und Nutzung ihrer Daten zu entscheiden. Opt-in-Lösungen sollten gesetzlich nur auf Basis ausdrücklicher Einwilligungen zulässig sein.
- Dies betrifft ebenso die Kennzeichnung hinsichtlich der (IT-) Sicherheit einschließlich der Deklaration der erwarteten und verpflichtenden Mitwirkung der Zahler. Es kann nicht allein die Aufgabe des Einzelnen sein, für (IT-) Sicherheit und Datenschutz zu sorgen, hierin liegt eine Grundaufgabe des Staates in der Daseinsvorsorge.
- Im Gesundheitsbereich sollten der Zweck und die Kriterien von Algorithmen auf gesetzlicher Basis transparent gemacht werden, wenn diese der Entscheidungsfindung z. B. bei der Festlegung einer Therapie usw. dienen. Nur dann können Nutzer ein ihnen eingeräumtes Widerrufsrecht überhaupt ausüben.
- Einfach nutzbare, valide Portale werden für sinnvoll erachtet, bei denen Verbraucherinnen und Verbraucher den Wert ihrer Daten einsehen können, um eine bessere Entscheidungsgrundlage für Einwilligungen zu erlangen. Analog zu Punkt 1 sollte die Einrichtung eines Instituts für die Zertifizierung von Portalen erfolgen.
- Apps, Software oder Websites, die die Privatsphäre- und Datenschutzeinstellungen der Endgeräte im Sinne der Verbraucher optimieren, sollten gefördert werden.
- Nutzerinnen und Nutzern ist ein Recht auf Auskunft und Offenlegung über die Verwertung personenbezogener Daten gesetzlich zu sichern.
- Verbraucherinnen und Verbrauchern ist das Recht auf Informationen darüber einzuräumen, wer bei der Nutzung von Online-Diensten, Wearables, Smartphones und weiteren digitalen Geräten personenbezogene Gesundheitsdaten verwertet.
- Es müssen Werkzeuge oder Technologien entwickelt werden, die es den Verbraucherinnen und Verbrauchern gestatten, den Wert der eigenen Daten abzuschätzen, um diese zu einem Verhandlungsgegenstand machen zu können.

4. Etablierung qualitativ hochwertiger Test-, Vergleichs- und Bewertungsportale

Empfehlungen:

- Es sind unabhängige valide Bewertungs- und Vergleichsportale sicher zu stellen, zu deren Qualität neben der Aussagekräftigkeit, Unabhängigkeit und Transparenz der Vergabe- bzw. Einstufungskriterien auch Vollständigkeit, Übersichtlichkeit, einfache Nutzung und klare Handlungsempfehlungen gehören. Von staatlicher Seite sind notwendige Sicherungen einzubauen, um überprüfen zu können, ob die definierten Qualitätsstandards eingehalten werden.

- Nach französischem Vorbild wäre daran zu denken, die Portale zur Offenlegung der folgenden Informationen zu veranlassen (1. Finanzierung – wer bezahlt die Kosten des Portals, 2. Provision – wer verdient beim Abschluss, 3. Haftung – für Fehlinformationen).
- Sinnvoll wäre es, staatlich geprüfte Qualitätsstandards einzuführen, beispielsweise in Form eines Vertrauenssiegels für Portale oder einer Zertifizierung bzw. in der Form von Audits. Wie unter Punkt 1 und 5 muss der Staat den Mut aufbringen, ein entsprechendes Portal / Institut zu finanzieren. Entsprechende Ansätze des BMJV in diese Richtung sind zu forcieren.
- Preisvergleichsportale sollten als „Gegenmaßnahme“ zu personalisierten Preisen einen Referenzpreis ausweisen.
- Digitale Informationen, Tests oder Produktvergleiche müssen einfachen und strengen Regeln von der Entstehung und Aufbereitung bis hin zur Publikation unterliegen, die laufend zu überprüfen sind (z. B. Information über Geschäftsmodell und finanzielle Beziehungen, insbesondere Provisionen, keine Werbung mit dem Stichwort „kostenlos“ oder ähnlich, wenn die Honorierung im Preis der verglichenen Produkte eingerechnet ist, keine Werbung mit dem Stichwort „preisgünstig“ oder ähnlich, wenn nicht alle Angebote am Markt einbezogen werden, öffentlich zugängliche Kriterien und Vergleichsmethoden, die durch Dritte nachprüfbar sind, Offenlegung, wie verglichen wird und welche Standards für welche Untersuchung zugrunde gelegt werden, Prüfung, ob die Aussagen eines Vergleichs maßgeblich für die wesentlichen Eigenschaften einer Finanzdienstleistung sind).

5. Durchsetzung einer datenschutzfreundlichen Technikgestaltung (privacy by design, privacy by default)

Empfehlungen:

- „Privacy by design”, Sicherheits-Defaults, einfache Verschlüsselungstechnologien und einfache Portabilität zur Vermeidung von Lock-in-Effekten sollten zum Grundstandard gehören und durch Regulierung oder Selbstregulierung gesichert werden.
- Die Zustimmungs- bzw. Widerspruchsmöglichkeiten zur Sammlung, Analyse und Weiterverkauf von Daten sollten durch datenschutzfreundliche Voreinstellungen unterstützt werden.
- Soweit möglich, sollten für Verbraucherinnen und Verbraucher nicht abschätzbare Risiken von vornherein ausgeschlossen werden. Nach dem Grundsatz: Im Falle einer Auswahl ist die jeweils sichere Option auch die einfache, naheliegende Option.
- Bei Datenschutzbehörden sind ausreichende Ressourcen und Instrumente bereitzustellen, insbesondere um „privacy by design“ und „privacy by default“ zu implementieren.

6. Effektive und effiziente Rechtsdurchsetzung

Empfehlungen:

- Formen kollektiver Rechtswahrnehmung, beispielweise durch Verbraucherorganisationen im Wege der Verbandsklage können Verbrauchern helfen, ihre Rechte zu identifizieren und durchzusetzen Die Einführung kollektiver Klageformen zur Bündelung gleichartiger Ansprüche, z.B. in Form einer Musterfeststellungsklage wird befürwortet
- Außergerichtliche Streitbelegungsmechanismen (Stichwort: Alternative Dispute Resolution oder Online Dispute Resolution) sollten weiter gestärkt werden, um eine schnellere Rechtsdurchsetzung zu erreichen. Sie sollten mit den Gerichten und den Behörden (BaFin, BNetzA) und den klagebefugten Verbraucherorganisationen strategisch verzahnt werden.
- Marktwächter Digitale Welt: das Zusammenspiel von staatlicher Aufsicht und Verbraucherschutz sollte verstetigt werden.
- Es wird ein enger Austausch zwischen Staat und Anbieterseite, Verbraucherorganisationen und der Netzgemeinde empfohlen, um sich gegenseitig zu informieren und Hinweise auf künftige Risiken zu erhalten.
- Ko-Regulierung in Form freiwilliger Standards und Branchenlösungen sollten dort erprobt werden, wo dies eine sinnvolle Ergänzung der staatlichen Regulierung darstellt. Dies kann insbesondere in Bereichen mit hoher Innovationsgeschwindigkeit und Dynamik, bei sehr heterogenen Nutzererwartungen und bei grenzüberschreitenden Fragen der Fall sein. Typische Anwendungsbeispiele wären Vereinbarungen über Transparenz-Grundsätze für Datennutzung oder Entwicklung eines Werte-Codex für die Big Data-Nutzung.
- Grundrechte und politikfeldübergreifende Regelungen sollten von der Ko-Regulierung strikt ausgeschlossen werden.
- Unabdingbar ist, dass vorab Mindestanforderungen hinsichtlich der Standardsetzung und -durchsetzung vereinbart und eingehalten werden („regulierte Ko-Regulierung“).
- Das Monitoring der Umsetzung könnten die Netzgemeinde, Marktwächter für die digitale Welt sowie Verbraucherorganisationen übernehmen.

7. Stärkung der digitalen Kompetenz

Empfehlungen:

- Kompetenzen im Umgang mit Digitalisierung sollten in allen Altersgruppen und sozialen Kontexten systematisch gefördert werden, um vulnerables Verhalten z. B. bei finanziellen oder gesundheitlichen Risiken zu minimieren.
- Verbraucherbildung muss digitale Kompetenzen vermitteln und für selbstbestimmte Datennutzung, Datensicherheit befähigen, dazu gehören u.a. konkrete Fertigkeiten und

Techniken der Anonymisierung und Verschlüsselung von Kommunikation, aber auch das Wissen um den Wert der eigenen Daten, das Kennen von Rechten und -pflichten in der digitalen Welt, die Einschätzung der Qualität und Neutralität von Portalen, Suchmaschinen und Labels.

- Die Anbahnung von Kompetenzen im Umgang mit Digitalisierung sollte bereits in der frühkindlichen und schulischen Bildung beginnen; gleichzeitig sollten für „Digital Immigrants“ diverse Formen des lebenslangen Lernens ausgebaut werden.
- Akteure der Zivilgesellschaft, wie z. B. der Chaos Computer Club, sollten auf allen Ebenen der formalen (schulischen), non-formalen (außerschulischen) und informellen (lebenslanges Lernen) Bildung als zusätzliche Akteure gewonnen werden, um z. B. schnell aktuelle Entwicklungen in der Digitalisierung aufgreifen zu.