SPD BUNDESTAGS FRAKTION

Die digitale Welt verbraucherfreundlich gestalten

Eckpunkte für eine moderne und durchsetzungsstarke Verbraucherpolitik

Die SPD steht für eine moderne und durchsetzungsstarke Verbraucherpolitik

Wir fordern:

1. **Stärkung und Ausbau der verbraucherbezogenen Forschung;**
2. die Einrichtung eines **Verbraucherpanels als** jährliche und repräsentative Verbrauchererhebung;
3. die Errichtung eines **Sachverständigenrates für Verbraucherfragen**;
4. **einen Verbrauchercheck im Rahmen von Gesetzgebungsverfahren**;
5. **Qualität bei der Verbraucherinformation** - die notwendigen und wesentlichen Informationen – aber auch die erforderlichen rechtsverbindlichen Einwilligungserklärungen – müssen dem genutzten Medium angemessen gestaltet und verständlich sein;
6. ein Recht auf **schnelles Internet für alle**, dass über eine Universaldienstverpflichtung gesetzlich absichert ist;
7. die gesetzliche Verankerung der **Netzneutralität**;
8. hohe Datenschutzstandards, damit die Persönlichkeitsrechte der Verbraucherinnen und Verbraucher gewahrt bleiben. Insbesondere setzen wir uns für eine **starke Europäische Datenschutz-Grundverordnung** ein (zur DS-GVO siehe auch Antrag der SPD-Fraktion BT-Drs. 17/11144),

    - nach der das so genannte **Marktortprinzip** zur Geltung kommt und somit bei der Verarbeitung von Daten europäischer Verbraucherinnen und Verbraucher auch europäisches Datenschutzrecht gilt;
    - in der am **Verbot mit Erlaubnisvorbehalt** und am **Einwilligungsvorbehalt** festgehalten wird. Begleitend müssen Wege gefunden werden, die Einwilligung im Hinblick auf die digitale Welt für datenverarbeitende Stellen und Verbraucherinnen und Verbraucher gleichermaßen praktikabler zu machen.
    - in der die Begriffe Profiling, Anonymisierung, Pseudonymisierung sowie Datenübertragung definiert werden;
    - die Datenschutz durch Technik und damit die Möglichkeiten der Anonymisierung und Pseudonymisierung fördert, mit dem Ziel, das Erheben von personenbezogenen Daten soweit möglich von vornherein zu vermeiden bzw. zu begrenzen.

- nach der die Zielvorgaben des Datenschutzes – Datensparsamkeit, Datenvermeidung und die Zweckbindung jeglichen Umgangs mit Daten – stärker zur Geltung kommen;
- die mit den Grundsätzen „**Privacy by default**“ und „**Privacy by Design**“ einen präventiven Ansatz des Datenschutzes fördert;
- die Regelungen zu **Profilbildung** etabliert, nach denen bereits bei der Erhebung der Daten und nicht erst bei deren Verarbeitung angesetzt wird und die die Souveränität der Betroffenen über ihre Daten bekräftigt;
- die Verbraucherinnen und Verbrauchern ein **Recht auf Datenportabilität** gewährt, das in keiner Hinsicht eingeschränkt werden darf sowie Regelungen zur Definition von einheitlichen Standards dafür trifft;
- die den rechtlichen Rahmen setzt, damit **gut ausgestattete und starke Aufsichtsbehörden** eine **konsistente Anwendung des Datenschutzrechts** in ganz Europa durchsetzen können;
- die durch spürbar hohe Strafen und Bußgelder finanzielle Anreize setzt, wirksame Datenschutz- und Datensicherheitsstandards in Unternehmen zu implementieren;

9. die seit Mai 2011 überfällige **Umsetzung der E-Privacy-Richtlinie**, die das Setzen von Cookies in der Regel unter Einwilligungsvorbehalt stellt;
10. **standardisierte Verfahren für Online-Bezahlmodelle**, so dass Verbraucherinnen und Verbraucher den Zahlungsdienstleister freie wählen können und so dauerhaft ein funktionierender Preis- und Leistungswettbewerb ermöglicht wird;
11. einen **Marktwächter digitale Welt**, der die Marktstrukturen beobachtet, Beschwerden von Verbraucherinnen und Verbrauchern sammelt und systematisch auswertet, Missstände an die zuständigen Aufsichtsbehörden meldet und im Zweifel auch die Rechte der Verbraucherinnen und Verbraucher durchsetzt. Darüber hinaus soll der Marktwächter in der Verbraucherbildung aktiv sein;
12. im Zuge der Einführung eines Marktwächters digitale Welt die Klarstellung im Unterlassungsklagegesetz (UKlaG), dass Datenschutzvorschriften, soweit sie Verbraucherrechte betreffen, Verbraucherschutzgesetze im Sinne des UKlaG sind;
13. die Möglichkeit von **Privatkopien** auch **in der digitalen Welt** zu erhalten;
14. die **Eindämmung von massenhaften Abmahnungen** von Urheberrechtsverletzungen durch Private, in dem eine Streitwertobergrenze mit klar gefasstem Anwendungsbereich eingeführt wird - insbesondere sind Ausnahmetatbestände mit unbestimmten Rechtsbegriffen abzulehnen. Auch der „fliegenden Gerichtsstands“ bei Urheberrechtsverstößen im Internet muss eingeschränkt werden.

Die digitale Welt verbraucherfreundlich gestalten

Einkaufen, Reisen buchen, Nachrichten lesen, mit Familie, Freunden und Bekannten über weite Entfernungen und Zeitgrenzen hinweg in Kontakt bleiben, sich an Bildern, Filmen, Büchern oder Musik erfreuen – online nicht nur bequem und schnell, sondern manchmal überhaupt erst möglich. Ein immer größerer Teil des Lebens verlagert sich ins Internet.

Die Digitalisierung globalisiert Verbraucherverhalten. Der Markt ist vielfältiger, aber auch unüberschaubarer und intransparenter, die rechtlichen und technischen Hintergründe sowie der Konsumalltag komplexer geworden. Viele Verbraucherinnen und Verbraucher finden sich im Tarifdschungel und im Kleingedruckten nicht zurecht.

Moderne Verbraucherpolitik muss die **Verbraucherinnen und Verbraucher** auch **in der digitalisierten Welt schützen**. Sie muss flexibel sein gegenüber verändertem Verbraucherverhalten sowie neuen Geschäftsmodellen und zugleich ein starkes und technikneutrales Fundament für die Rechte der Verbraucherinnen und Verbraucher bieten.

Moderne Verbraucherpolitik muss die **Grundrechte der Verbraucherinnen und Verbraucher auch in der digitalen Gesellschaft** durchsetzen. Hierzu zählen der Datenschutz im Internet sowie eine angemessene Grundversorgung mit schnellem Internet und ein neutrales und diskriminierungsfreies Netz, das keine Inhalte oder User bevorzugt. Die Möglichkeiten der anonymen Nutzung des Internets sollten den Verbraucherinnen und Verbraucher und nicht Kriminellen dienen. Zudem muss ein effektiver Kinder- und Jugendschutz im Internet etabliert werden.

Sozialdemokratische Verbraucherpolitik bedeutet heute **ganzheitliche Verbraucherpolitik**, die Verbraucherschutz als Antrieb für moderne Politik auch in anderen Politikfeldern betrachtet. Verbraucherinnen und Verbraucher sind der Motor der Wirtschaft. Sie sind Teil einer zukunftsfähigen Wirtschaftspolitik, die für fairen Wettbewerb sorgt und verantwortungsvolle Anbieter stärkt.

Moderne Verbraucherpolitik muss Verbraucherinnen und Verbraucher verstehen

Die Digitalisierung bringt Veränderungen für Verbraucherinnen und Verbraucher mit sich, die Eingang in die weitere Verbraucherschutzdiskussion finden müssen. Verbraucherschutzpolitik steht mit der Digitalisierung vor einer neuen Herausforderung. Einerseits gilt es die technischen Errungenschaften zu nutzen, andererseits müssen die Interessen der Verbraucherinnen und Verbraucher gewahrt werden. Die Schutzwürdigkeit von Verbraucherinnen und Verbrauchern muss unter zwei Maßgaben besondere Beachtung finden:

- Verbraucherinnen und Verbraucher, die über vernetzte Endgeräte interagieren, haben kein persönliches Gegenüber, dessen Aktionen und Reaktionen sie einschätzen und bewerten können.

- Das Kenntnisniveau und die Umgangserfahrenheit mit neuen Medien sind unter Verbraucherinnen und Verbrauchern unterschiedlich ausgeprägt. Das jeweilige Schutzniveau muss so angesiedelt sein, dass es alle Verbraucherinnen und Verbraucher erfasst.

Eine wesentliche Veränderung der Digitalisierung ist die fehlende face-to-face Kommunikation, die neue Wege erfordert, um den Wahrheits- und Aussagegehalt einzelner Aussagen zu erkennen. So können Verbraucherinnen und Verbraucher bei Bewertungsportalen nicht erkennen, wer die Bewertungen geschrieben hat. Sie können beispielsweise nicht erkennen, ob es sich bei Bewertungsportalen um Guerilla-Marketing handelt oder um Verbraucherinnen und Verbraucher mit gleichgelagerten Interessen. Das „Mehr“ an Transparenz, das das Internet grundsätzlich zu bieten im Stande ist, kann so für Verbraucherinnen und Verbraucher schnell zum Irrgarten werden.

Moderne Verbraucherpolitik muss sich in der digitalen wie auch in der analogen Welt an den tatsächlichen Bedürfnissen der Verbraucherinnen und Verbraucher orientieren. Aktuelle empirische Studien zum Verbraucherverhalten, Gutachten und Stellungnahmen des Wissenschaftlichen Beirats Verbraucher- und Ernährungspolitik beim Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) sowie aktuelle Arbeiten und Positionen des Europäischen Parlaments zum Thema "vulnerable consumers" bieten eine gute Grundlage für ein modernes Verbraucherleitbild, nach dem es „die“ Verbraucherinnen und Verbraucher oder „den“ Entscheidungstyp nicht gibt. Jede Verbraucherin und jeder Verbraucher hat besondere Kenntnisse. Während eine Verbraucherin Ernährungsexpertin ist, ist ein anderer Verbraucher Computerspezialist.

Wir vertreten ein differenziertes Verbraucherleitbild, wonach sich Verbraucherinnen und Verbraucher grob in drei Kategorien einordnen lassen:

- den „verletzlichen“ Verbraucher, der mit der Angebotsvielfalt und -unübersichtlichkeit überfordert ist,

- den „vertrauenden“ Verbraucher, der aus verschiedensten Gründen (z.B. Zeitmangel, Bequemlichkeit o.Ä.) auf die Sicherheit der Produkte und die Seriosität des Angebots vertraut,

- und den „verantwortungsvollen“ Verbraucher, der sich vor einer Entscheidung informiert und bewusst auswählt.

In allen Verbraucherinnen und Verbrauchern steckt ein wenig von jedem Verbrauchertypus. Verbraucherpolitik muss diese unterschiedlichen Realitäten im Alltag der Verbraucherinnen und Verbraucher berücksichtigen und passgenaue Antworten finden.

Um den verschiedenen Verbrauchertypen gerecht zu werden, muss es Ziel der Marktgestaltung werden, dass gesunder Menschenverstand ausreichend ist, um bewusste Entscheidungen zu treffen.

Als Grundlage einer Politik, die allen Verbraucherinnen und Verbrauchern gerecht wird, ist der Ausbau und die stärkere Berücksichtigung von **verbraucherbezogener Forschung** erforderlich. Nur durch valide Erkenntnisse – etwa der Verhaltensökonomie oder zu Marktstrukturen – kann Verbraucherpolitik den Markt so gestalten, dass auch verletzliche und vertrauende Verbraucherinnen und Verbraucher nicht benachteiligt oder überfordert werden.

Ein Baustein für ein besseres Verständnis von Verbraucherinnen und Verbrauchern ist ein **Verbraucherpanel**. Wir fordern eine als Wiederholungsbefragung konzipierte jährliche und repräsentative Verbrauchererhebung, die anhand konkreter Fragestellungen und sowohl die digitale als auch die analoge Welt berücksichtigend zur Marktlage in den verschiedenen Konsumfeldern valide Daten etwa zur Informationslage, zur Transparenz oder zum Verhalten von Verbraucherinnen und Verbrauchern in Bezug auf konkrete Konsumentscheidungen liefern kann.

Ein weiterer Baustein ist die Errichtung eines **Sachverständigenrates für Verbraucherfragen**. Dieser hat die Aufgabe, sowohl Gutachten über die Situation der Verbraucherinnen und Verbraucher in Deutschland als auch solche zu einzelnen Problemen von Verbraucherinnen und Verbrauchern periodisch zu erstellen und mit den gewonnenen Erkenntnissen die Bundesregierung zu beraten und ihr Lösungsvorschläge zu unterbreiten. Daneben soll der Sachverständigenrat auch zu aktuellen Themen Stellungnahmen und Empfehlungen abgeben.

Darüber hinaus wollen wir, dass gesetzgeberische Entscheidungen zukünftig einem **Verbrauchercheck** unterzogen werden, der die Auswirkungen von gesetzlichen Regelungen auf Verbraucherinnen und Verbraucher in der analogen wie auch digitalen Welt beleuchtet. Es soll benannt werden, ob das gesetzgeberische Vorhaben Verbraucherinnen und Verbraucher nutzt, dieser Nutzen sodann konkret ausgeführt werden und gegebenenfalls eine Frist zur Evaluation gesetzt werden.

„Information Overkill“ – Qualität statt Quantität bei Verbraucherinformationen

Das Internet bietet Verbraucherinnen und Verbrauchern schier unendliche Möglichkeiten sich zu informieren, z.B. über Händler- und Anbieterseiten, Bewertungsportale, soziale Netzwerke und Foren. In den vergangenen Jahren sind zudem immer mehr Informationspflichten gesetzlich festgeschrieben worden. Diese sind nicht nur für Unternehmen oftmals eine Belastung, sondern für Verbraucherinnen und Verbraucher mittlerweile in vielen Fällen unüberschaubar.

Informationspflichten sind aus verbraucherpolitischer Perspektive nur dann sinnvoll, wenn sie einen Mehrwert für Verbraucherinnen und Verbraucher bieten. Der Nutzen für die Verbraucherinnen und Verbraucher wird derzeit nicht ausreichend evaluiert. Verbraucherinnen und Verbraucher sollen die richtige Information zum richtigen Zeitpunkt in einer für sie verständlichen Weise erhalten. Daher muss bezüglich derzeit bestehender aber auch vor der Einführung neuer Informationspflichten geprüft werden:

Was sind Ziel und Zweck der Information?

Ist eine Information für den angestrebten Zweck das richtige Mittel oder anders gefragt, handelt es sich um einen Bereich, in dem eine Information den Verbraucherinnen und Verbrauchern die Wahlfreiheit erleichtert und somit einen Mehrwert bietet oder eher um einen Bereich in dem Verbraucherinnen und Verbraucher schutzbedürftig sind und daher andere Instrumente zielführender wären?

Ist sie verfügbar, wenn sie wirklich benötigt wird und wie kann dies im Kontext der digitalen Welt – so ist beispielsweise die Darstellungsform auf mobilen Endgeräten mit ihren vergleichsweise kleinen Displays zu berücksichtigen – optimiert werden?

Ist die Information auch für die unterschiedlichen Verbrauchergruppen verständlich und wirksam?

Am Ende müssen Verbraucherinformationen so konzipiert sein, dass die notwendigen, wesentlichen Informationen – aber auch die erforderlichen rechtsverbindlichen Einwilligungserklärungen – dem genutzten Medium angemessen gestaltet und verständlich sind.

Das Netz und Ich – Meine Grundrechte in der digitalen Welt

Ob die digitale Gesellschaft eine offene, demokratische, kreative, verbraucherfreundliche sowie eine innovative und wirtschaftlich erfolgreiche sein kann, entscheidet sich nicht zuletzt daran, ob es gelingt das Internet offen und diskriminierungsfrei zu halten. Grundlage hierfür ist, dass alle Bürgerinnen und Bürger, alle Verbraucherinnen und Verbraucher Zugang zu schnellem Internet haben sowie eine gesetzlich verankerte Netzneutralität.

Recht auf schnelles Internet

Die Digitalisierung der Gesellschaft ermöglicht es den Menschen beispielsweise im Bereich der Bürgerbeteiligung oder der Art der Informationsbeschaffung und Kommunikation neue Wege zu gehen. Unser Ziel ist deshalb ein Recht auf ein schnelles Internet für alle, auch in ländlichen Räumen. Wir wollen eine digitale Spaltung der Gesellschaft vermeiden bzw. überwinden.

Der flächendeckende Breitbandausbau schafft die Voraussetzungen für die Teilhabe aller Bevölkerungsgruppen und Regionen am Fortschritt und an den Möglichkeiten der digitalen Gesellschaft. Breitbandversorgung gehört zur Daseinsvorsorge. Keine Verbraucherin und kein Verbraucher, keine Bürgerinnen und kein Bürger darf hiervon ausgegrenzt werden. Die flächendeckende Versorgung mit schnellem Internet soll daher über eine Universaldienstverpflichtung gesetzlich abgesichert werden.

Gesetzlich verankerte Netzneutralität

Kern der Netzneutralität ist der Gleichheitsgrundsatz. Netzneutralität fordert die Gleichbehandlung aller Daten im Internet unabhängig von kommerziellen Interessen oder sonstigen monetären oder andersgearteten Bevorzugungen. Der gleichberechtigte Transport von Daten und der diskriminierungsfreie Zugang zu Inhalten sind für optimale Teilhabe und niedrige Marktzugangsschwellen konstitutiv. Die Diskriminierungsfreiheit der Infrastrukturen und Inhalte bilden die Grundlage für ein freies und innovationsfreundliches Internet.

Für Verbraucherinnen und Verbraucher bedeutet ein neutrales Netz, dass sie unabhängig von Anwendung, Dienstleistung oder Inhalt sowie unabhängig von der Adresse des Senders oder des Empfängers gegenüber ihrem Zugangsprovider einen Anspruch auf diskriminierungsfreie Internetnutzung haben. Ein neutrales Netz ist auch die Grundlage für einen funktionierenden und diskriminierungsfreien Markt in den Bereichen Online-Dienstleistungen, Online-Inhalte und Online-Anwendungen. Eine bevorzugte Übermittlung

bestimmter Datenpakete schränkt den freien Wettbewerb ein und fördert Monopolstrukturen. Dies schadet nicht nur dem wirtschaftlichen Potential des Internets, sondern auch den Verbraucherinnen und Verbrauchern.

Es ist daher eine gesetzliche Verankerung der Netzneutralität erforderlich. Der Datentransport muss nach dem so genannten Best-Effort-Prinzip erfolgen. Auch das so genannte Any-to-any-Prinzip soll festgeschrieben werden, wonach jeder grundsätzlich Zugang zu jedem Inhalt im Internet haben und Inhalte selbst anbieten kann.

Persönlichkeitsschutz im Netz – das Grundrecht auf informationelle Selbstbestimmung und das IT-Grundrecht

Jeder hat das Recht selbst zu entscheiden, was er wann mit seinen personenbezogenen Daten macht und wie diese Daten verarbeitet werden. Das Grundrecht auf informationelle Selbstbestimmung schützt vor Zugriff auf einzelne personenbezogene Daten des Betroffenen.

In der heutigen Zeit immer wichtiger ist auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – das IT-Grundrecht. Es schützt vor dem potentiellen Zugriff auf eine Vielzahl von (personenbezogenen) Daten (Datenbestand), die auf einem informationstechnischen System gespeichert sind und ist bereits anwendbar, wenn auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden könnten. Es schützt also das Interesse des Nutzers, dass die auf dem Laptop, Mobiltelefon, Tablet oder der Cloud erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben, indem bereits ein Zugriff auf das Gerät z.B. über einen Trojaner verboten ist, ohne das es tatsächlich zu einem Zugriff auf Daten kommen muss.

Maßnahmen des Datenschutzes und der Datensicherheit sind besonders wichtige Mittel und ergänzen sich gegenseitig, um den Schutz dieser Grundrechte zu gewährleisten. Hohe Datenschutzstandards sind mehr denn je notwendig, insbesondere weil Verbraucherinnen und Verbraucher immer mehr digitale Technik nutzen und somit immer mehr digitale Spuren hinterlassen, aber auf Grund der immer komplexeren Systeme meist nicht in der Lage sind, ausreichende Selbstschutzmaßnahmen zu ergreifen. Hohe Datenschutz- und Datensicherheitsstandards schaffen das nötige abstrakte Vertrauen in diese Techniken und ermöglichen erst dadurch allen Verbraucherinnen und Verbraucher unabhängig von den eigenen Kenntnissen und Fähigkeiten einen unbefangenen Umgang mit den neuen Techniken und Möglichkeiten. Hohe Datenschutz- und Datensicherheitsstandards tragen auf diese Weise auch dazu bei, dass alle Verbraucherinnen und Verbrauchern unabhängig von ihren technischen Kenntnissen an den neuen Entwicklungen teilhaben können.

Datenschutz ist Verbraucherschutz

Digitale Herausforderungen an den Datenschutz

Die Anforderungen an einen wirksamen Datenschutz haben sich durch die zunehmende Nutzung digitaler Techniken verändert. Datenschutz – und somit der Schutz der informationellen Selbstbestimmung der Verbraucherinnen und Verbraucher – lässt sich nicht mehr allein dadurch gewährleisten, dass auf problematische Sachverhalte im Einzelfall gesetzgeberisch reagiert wird. Es sind nicht mehr nur Datenhandel, die Datensammelwut des Staates oder einzelner Unternehmen, illegale Geschäftspraktiken oder in einzelnen Techniken liegende funktionale Besonderheiten, die die Souveränität der Verbraucherinnen und Verbraucher über ihre Daten gefährden. Aus der rasanten Entwicklung neuer Techniken, der Globalisierung von Datenverarbeitung und der Vernetzung sämtlicher Lebensbereiche sowie der Verknüpfung von Alltagsgegenständen mit dem Internet ergeben sich vielmehr auch strukturelle Risiken für die Grundrechte der Betroffenen. Diese Entwicklung wird in den kommenden Jahren zunehmen.

Profilbildung – Big Data, Tracking und Identifyer

Profilbildung – das Erfassen von Verhalten und Persönlichkeitsmerkmalen zur Berechnung von Vorlieben oder Wahrscheinlichkeiten – ist in vielen Bereichen der digitalisierten Gesellschaft bereits Realität. Im Internet, so etwa in Sozialen Netzwerken oder Suchmaschinen, aber auch durch das Setzen von Cookies oder durch andere vielfältig nutzbare technische Mittel, wird das Surfverhalten ausgewertet, um beispielsweise gezielt Werbung platzieren zu können. Bei mobilen Endgeräten kommt die Möglichkeit der Auswertung von Geodaten hinzu. Das Smartphone sagt seinem Besitzer oder seiner Besitzerin, ob ein nahegelegenes Geschäft gerade ein Sonderangebot hat, das ihn interessieren könnte oder wo er seinen Lieblingskuchen essen kann. Diese auf Profilbildung basierenden Dienste können nützliche Helfer im Alltag sein und Verbraucherinnen und Verbraucher mit gewünschten Informationen versorgen.

Kostenlos, aber nicht umsonst: Die meisten Dienste im Internet kosten kein Geld; umsonst sind sie dennoch nicht. Verbraucherinnen und Verbraucher müssen besser über den „Preis“ aufgeklärt werden, den sie für die „kostenlose“ Nutzung von sozialen Netzwerken oder Suchmaschinen, bestimmter Apps, Spiele oder Messenger-Dienste bezahlen. Die Wirtschaftlichkeit kostenloser Angebote im Internet hängt unmittelbar mit der Verarbeitung der persönlichen Daten der Nutzerinnen und Nutzer zusammen. Je umfangreicher und valider die Daten der Nutzerinnen und Nutzer sind, desto besser und gewinnbringender lassen sich diese z.B. für personalisierte Werbung verwenden. Wir müssen Wege finden, um

sicherzustellen, dass Verbraucherinnen und Verbraucher darüber informiert sind, dass ihre Daten mit einer Monetarisierungsstrategie weiterverwendet werden. Nur wenn Verbraucherinnen und Verbraucher die Geschäftsmodelle hinter dem scheinbar kostenlosen Angebot verstehen, können sie abgewogene Entscheidungen darüber treffen, welche Dienste sie nutzen und welche Daten sie innerhalb dieser Dienste preisgeben wollen.

So werden personenbezogene Daten in einem Umfang und in einer Vielfalt gesammelt und ausgewertet, die nicht von allen Verbraucherinnen und Verbrauchern gewollte Einblicke in wesentliche Teile der Lebensgestaltung oder gar aussagekräftige Bilder der Persönlichkeit ermöglichen. Neben einer verbesserten Aufklärung der Verbraucherinnen und Verbraucher über die Notwendigkeit und die Möglichkeiten des Selbstdatenschutzes, bedarf es allgemeingültiger Regelungen, unter welchen Voraussetzungen Profilbildung erlaubt sein soll.

Cookies

Während sich das Speichern von einfachen Cookies – kleiner Textdateien über das Surfverhalten nachverfolgt wird - auf dem eigenen Rechner durch entsprechende Einstellungen im Browser noch einigermaßen steuern lässt, benutzen immer mehr Trackingdienste sogenannte Flash Cookies. Diese werden bisher von keinem Browser angezeigt, so dass auch keine Möglichkeit zum Löschen besteht. Hierfür ist eine Spezialsoftware nötig. Verbraucherinnen und Verbraucher, die diese Dienste oft nicht einschätzen können und deren Browser ihnen nicht einmal die Existenz dieser Flash-Cookies anzeigt, werden sich jedoch nicht veranlasst sehen, eine solche Spezialsoftware zu verwenden.

Die Erstellung von Nutzerprofilen erfolgt nicht immer nur durch den Anbieter der von den Nutzerinnen und Nutzern besuchten Webseite selbst, der durch die bereitgestellte Datenschutzerklärung einen Ansprechpartner für die Ausübung des Wahlrechts der Nutzerinnen und Nutzer hinsichtlich der Datenerhebung und -verwendung transparent machen kann, sondern oft und sehr umfangreich auch durch Dritte. Mangels Transparenz ist es Nutzerinnen und Nutzern in solchen Fällen häufig nicht möglich, Einfluss auf die Erhebung und spätere Verwendung der Daten zu nehmen.

Die seit Mai 2011 überfällige Umsetzung der E-Privacy-Richtlinie[1], die das Setzen von Cookies in der Regel unter Einwilligungsvorbehalt stellt, muss unverzüglich erfolgen (siehe Gesetzentwurf der SPD-Fraktion BT-Drs. 17/8454). Die behaupteten Schwierigkeiten bei der Umsetzung bestehen nicht, wie sich in anderen EU-Mitgliedstaaten gezeigt hat. Ebenso stellt die Selbstverpflichtung des Deutschen Datenschutzrats Online-Werbung, nach der externe

[1] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der elektronischen Kommunikation (ABl. L 201 vom 31.7.2002, S. 37).

Werbeanbieter ihre Werbung mit einem Symbol kennzeichnen sollen, wenn sie Technologien zur Nachverfolgung der Nutzer verwenden, keine gleichwertige Umsetzung dar.

Radio Frequency Identification – RFID Chips

RFID-Chips sind kleine Funkchips, die in oder an Produkten angebracht werden. Sie dienen meist dazu, dass Händler die Lieferkette besser nachverfolgen und die Logistik optimieren können. Für Kundinnen und Kunden sind RFID-Chips in der Regel nicht sichtbar. Auf den Chips ist eine eineindeutige Nummer gespeichert, die über Funk aus bis zu acht Metern mit beliebigen Lesegeräten desselben Standards – von Verbraucherinnen und Verbrauchern unbemerkt – ausgelesen werden kann. Eine technische Beschränkung der Auslesbarkeit auf bestimmte oder einzelne Lesegeräte ist nicht möglich.

Die EU-Kommission geht davon aus, dass bis 2015 weltweit ca. 25 Mrd. Produkte über Funkverbindungen verfügen werden. Das Mitführen dieser Chips durch Verbraucherinnen und Verbraucher kann personenbezogene oder personenbeziehbare Daten erzeugen. So können beispielsweise RFID-Chips in Einkaufswagen die von der ihn schiebenden Person gekauften Produkte erfassen. Sie können ebenso feststellen, nach welchem Muster eine Person sich durch ein Geschäft bewegt und wie lange sie vor einem bestimmten Regal stehen bleibt. Wird bei der Bezahlung eine Kundenkarte verwendet oder erfolgt die Bezahlung mittels EC- oder Kreditkarte, können die gewonnenen Erkenntnisse einer bestimmten Person zugeordnet werden. Von dieser Person kann dann nicht nur ein Bewegungsprofil im Geschäft, sondern auch ein Profil über die Konsumgewohnheiten erstellt werden. Auch können bei einer Erfassung über einen längeren Zeitraum Änderungen im Konsumverhalten der Kundin oder des Kunden festgestellt werden, die über Veränderungen in anderen Lebensbereichen Aufschluss geben. So kann beispielsweise anhand des Warenkorbs auf Schwangerschaften oder Allergien geschlossen werden.

Diese Form der Profilbildung ist nach derzeit geltendem Datenschutzrecht nicht erlaubt. Wir setzen uns dafür ein, dass auf europäischer Ebene starke Regelungen zum Schutz vor Profilbildung Eingang in die geplante Datenschutz-Grundverordnung (DS-GVO) finden. Das Grundrecht auf informationelle Selbstbestimmung muss bei der Verwendung von RFID-Technologien im Endkundenbereich gewährleistet bleiben.

Verbraucherinnen und Verbraucher müssen zudem über den Einsatz von RFID informiert werden und Produkte, die Chips enthalten, müssen gekennzeichnet werden. Darüber hinaus wollen wir, dass eine nicht umkehrbare Deaktivierung der Chips erfolgt, sobald ein Produkt die Handelskette verlässt, oder die Chips physisch entfernt oder zerstört werden. Sollte eine verpflichtende regulierte Selbstregulierung der Wirtschaft unter Beachtung der Empfehlungen der EU-Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen nicht zeitnah oder

nicht ausreichend schlagkräftig zustande kommen, so müssen die Persönlichkeitsrechte der Verbraucherinnen und Verbraucher gesetzlich abgesichert werden.

Big Data und Ubiquitous Computing

Der Begriff **Ubiquitous Computing** bezeichnet einen Zustand der allgegenwärtigen rechnergestützten Informationsverarbeitung. Nachdem in den 70er Jahren Großrechner und seit den 90er Jahren die Personal Computer die Philosophie des Datenschutzes prägten, geht die Entwicklung dahin, dass die den Menschen umgebenden Alltagsgegenstände untereinander vernetzt werden und Informationen austauschen. Hierbei entstehen bislang ungeahnte Datenmengen. Neue Trends, wie die unter dem Stichwort **„Big Data“** bekannten Technologien zur Verknüpfung und Auswertung solcher unstrukturierter Datenmengen aus verschiedensten Quellen – teils in Echtzeit -, stellen den Datenschutz vor Herausforderungen.

Big Data Technologien bieten Chancen. Sie können etwa im Gesundheitsbereich (z.B. in der Krebsforschung und -behandlung) oder in der Verkehrsplanung wertvolle Erkenntnisse liefern. Das Gelingen einer echten Energiewende wird auch davon abhängen, ob bedarfsgerechte Energieversorgung mittels intelligenter Stromnetze und Stromzähler in den Haushalten (Smart grids und Smart meter) oder intelligenter Haushaltsgeräte, die sich dann einschalten, wenn genug grüner Strom verfügbar ist, gewährleistet werden kann. Auf der anderen Seite laufen Verbraucherinnen und Verbraucher Gefahr, dass Unternehmen in nie gekannter Weise Einblick in wesentliche Teile ihrer Lebensgestaltung gewinnen und aussagekräftige Bilder ihrer Persönlichkeit erhalten. Bei der Auswertung der Daten, etwa von intelligenten Stromzählern, kann theoretisch festgestellt werden, wann einzelne Verbraucherinnen und Verbraucher kochen, waschen, schlafen, zu Hause oder im Urlaub sind, ob sie morgens ein hart oder weichgekochtes Ei essen oder zu welcher Uhrzeit sie (sogar welche) Fernsehsendung schauen. Es gilt, den gesellschaftlichen Nutzen der Datenverarbeitung von Big Data Technologien mit dem Recht auf informationelle Selbstbestimmung zu vereinen. Datenschutz ist ein grundlegendes Freiheitsrecht. Jede und jeder muss selbst entscheiden können, wie mit ihren/seinen Daten umgegangen wird. Daher kommt auch hier Datenschutz durch Technik eine grundlegende Bedeutung zu: Anonymisierung und Pseudonymisierung können einen wichtigen Beitrag dazu leisten, Datenanalysen mit den Zielen und den hohen Anforderungen des Datenschutzes vereinbar zu machen. Diese Vereinbarkeit ergibt sich allerdings nicht von alleine – sie muss aktiv politisch gestaltet werden. Vor diesem Hintergrund müssen klare gesetzliche Regelungen bereits beim Erheben von personenbezogenen Daten ansetzen und nicht erst bei deren Nutzung.

Es muss sichergestellt werden, dass der unbestreitbare Nutzen, den z.B. Big Data-Anwendungen für die Gesellschaft bringen können, nicht zu gläsernen Verbraucherinnen und Verbrauchern führt. Der anonymen Gestaltung von auf Profilbildung basierenden

Geschäftsmodellen und der Förderung entsprechender Techniken kommt dabei besondere Bedeutung zu. Auf Grund der weitreichenden Einblicke in die Persönlichkeit und die Lebensführung ist Profilbildung ohne die Einwilligung der betroffenen Verbraucherinnen und Verbraucher abzulehnen. Unzulässige Profilbildung sollte hart sanktioniert werden.

IPv6 – Das neue Internetprotokoll

Onlinefähige Mobilgeräte werden von immer mehr Menschen genutzt, weshalb der Bedarf an IP-Adressen stetig zunimmt. In absehbarerer Zeit wird daher der heute für die Vergabe von IP-Adressen genutzte IPv4 Standard, mit dem lediglich ca. 4,3 Mrd. Nummernblöcke verteilt werden können, durch den neuen IPv6 Standard ersetzt. Nach diesem Standard kann jeder Quadratmillimeter Erdoberfläche mit $6{,}65 * 10^{38}$ IP-Adressen ausgestattet werden.

Beim IPv4 Standard hat u.a. die Adressknappheit dazu geführt, dass Verbraucherinnen und Verbraucher dynamische, also bei jeder Einwahl ins Internet andere IP-Adressen bekamen. Durch die Vielzahl der Adressen im IPv6 Standard entsteht die Möglichkeit, Verbraucherinnen und Verbrauchern eine statische, also eine dauerhafte IP-Adresse zuzuteilen. Dies hätte für die Verbraucherinnen und Verbraucher und ihr Recht auf informationelle Selbstbestimmung unangenehme Folgen. Denn dadurch würde es Webseitenbetreibern ermöglicht, jede Nutzerin und jeden Nutzer zweifelsfrei wiederzuerkennen. Webtracking und Profilbildung würden enorm vereinfacht und ausgebaut. Auch im Bereich der Bestandsdatenauskunft und der Vorratsdatenspeicherung ist diese Entwicklung von Bedeutung.

Doch auch wenn die dynamische Verteilung der IP-Adressen beibehalten wird, besteht die Gefahr, dass Verbraucherinnen und Verbraucher bei wiederkehrendem Besuch einer Website oder eines Netzwerkes erkannt werden. Denn ein Bestandteil der neuen IPv6-Adressen ist die Nummer der Geräte, mit der sich Verbraucherinnen und Verbraucher im Netz bewegen. Dem könnte durch sogenannte „Privacy Extensions“ begegnet werden, die bei elektronischen Geräten als standardmäßige Datenschutzerweiterung verhindern, dass die Gerätenummer als Bestandteil der IP-Adresse verwendet wird.

Bei der notwendigen Umstellung auf den IPv6 Standard sollte sichergestellt werden, dass bereits bei der Entwicklung der dafür notwendigen Techniken Datenschutzanforderungen berücksichtigt werden. Hier sind verbindliche Vorgaben zu Datenschutz- und Datensicherheitsmaßnahmen von Nöten, an die sich die Internet-Service-Provider (ISP) halten müssen.

ISP sollten Verbraucherinnen und Verbrauchern eine Wahlmöglichkeit belassen, ob diese dynamische oder statische IP-Adressen haben möchten. In jedem Fall müssen die Verbraucherinnen und Verbraucher rechtzeitig und umfassend darüber informiert werden, wenn ihr Internetanbieter auf IPv6 umstellt.

Gerätehersteller sollten Privacy Extensions bei Endkunden-Systemen standardmäßig aktivieren. Wird dies nicht gewährleistet, sollte eine entsprechende Verpflichtung auch gesetzlich verankert werden.

Cloud-Dienste

Bei der Nutzung von Cloud-Diensten wird auf der Seite der Nutzerinnen und Nutzer ein Teil der benötigten Hardware oder Software nicht mehr selbst bereitgestellt, sondern bei einem Anbieter gemietet. Beispielsweise die mittels Handykamera aufgenommenen Fotos, die über das Smartphone gehörte Musik oder auch die Software zur Bearbeitung von Daten der Nutzerinnen und Nutzern sind dann nicht mehr auf dem Telefon selbst gespeichert. Sie befinden sich stattdessen in den weltweit verteilten Rechenzentren der Cloud-Anbieter auf deren Servern. Nutzerinnen und Nutzer haben trotz der räumlichen Ferne über ihr Endgerät Zugriff auf die Daten. Die Daten liegen bildlich gesprochen in einer Wolke (englisch *cloud*) irgendwo im Internet. Dies kann mit Blick auf die Datensicherheit von Vorteil, aber auch mit erheblichen nachteiligen Folgen verbunden sein.

Die Rechte der Nutzerinnen und Nutzer von Cloud-Diensten und die Pflichten der Anbieter sind diffus. Es herrscht große Rechtsunsicherheit. Zunächst ist nicht immer nur das rechtliche Verhältnis zwischen Cloud-Nutzerinnen und Nutzern und Cloud-Anbieter entscheidend. Häufig nutzt ein Cloud-Anbieter wiederum die Dienste eines anderen Cloud-Anbieters, so dass rechtliche Dreiecksverhältnisse entstehen. Solche Dreiecksverhältnisse gibt es auch, wenn Verbraucherinnen und Verbraucher SaaS-Dienste (Software as a Service) nutzen. Der Anbieter des Software-Dienstes nutzt selbst häufig die technische Infrastruktur eines weiteren Cloud-Anbieters, sog. IaaS-Dienste (Infrastructure as a Service). Hinzu kommen Rechtsunsicherheiten, die daraus entstehen, dass die Daten der Nutzerinnen und Nutzer in verschiedenen Ländern, insbesondere außerhalb der EU, verarbeitet werden und sich somit die Frage nach dem anwendbaren Recht stellt. Nutzerinnen und Nutzer stehen hier häufig vor Problemen, wenn sie ihre Rechte z.B. auf Löschung von Daten durchsetzen wollen.

Neben den rechtlichen Unsicherheiten lässt sich im Zusammenhang mit Cloud-Diensten auch ein Defizit an Transparenz gegenüber Nutzerinnen und Nutzern feststellen. Diese wissen häufig nicht einmal, dass sie Daten in der Cloud speichern und wo die Datenverarbeitung erfolgt. Nutzerinnen und Nutzer gehen häufig davon aus, dass die Fotos, die sie mit ihrem Smartphone aufnehmen, auf dem Telefon selbst gespeichert werden. Oft ist aber bereits per Voreinstellung die Speicherung in der Cloud aktiviert. Ebenso ist oft nicht ersichtlich, ob die Daten der Nutzerinnen und Nutzer durch den Cloud-Anbieter noch zu anderen Zwecken verarbeitet werden, wie z.B. zu Werbezwecken.

Wir wollen, dass die technischen Standards und der Umgang mit Daten von Verbraucherinnen und Verbrauchern nachvollziehbar und kontrollierbar sind. Dies kann beispielsweise mittels Datenschutz- und Datensicherheitsaudits erreicht werden. Cloud-Anbieter sollten zudem Transparenz darüber gewährleisten, in welche Länder sie Daten

übermitteln. Gesetzlich verankert werden sollte auch, dass ohne Einwilligung der Verbraucherinnen und Verbraucher keine Übermittlung in Länder außerhalb der EU erfolgen darf, die entweder ein niedrigeres Datenschutzniveau haben oder in denen Behörden auf die Daten Zugriff nehmen können. Zudem muss auch bei Cloud-Diensten der Grundsatz der Zweckbindung der Datenverarbeitung beachtet werden. Wir setzten uns darüber hinaus für die Schaffung von internationalen Standards für Cloud-Dienste ein.

Chancen realisieren – Risiken minimieren

Damit sich für Verbraucherinnen und Verbraucher, die Wirtschaft und die Gesellschaft insgesamt die **Chancen der Digitalisierung realisieren** und nicht die Risiken, muss moderne Verbraucherpolitik die Entwicklungen beobachten, Trends frühzeitig erkennen und diese in die richtigen Bahnen lenken.

Zur Lösung gegenwärtiger Probleme, aber auch als Basis für alle kommenden Entwicklungen in der digitalen Welt, benötigen wir einen **hohen Standard an Datenschutz und Datensicherheit**. Wir brauchen ein **technikneutrales Datenschutzrecht**, dass unabhängig vom genutzten Medium für den Umgang mit Daten allgemeingültige Regeln schafft. Dieses muss die mit der Digitalisierung der Gesellschaft bislang einhergegangenen Veränderungen aufnehmen und zugleich gegenüber zukünftigen neuen Techniken und Geschäftsmodellen flexibel bleiben. Große Bedeutung wird hierbei dem technischen Datenschutzschutz – privacy by design und privacy by default – zukommen, indem der Datenschutz bereits bei der Entwicklung von Diensten und Geräten implementiert wird.

Die hohen Standards müssen auch **grenzüberschreitend** gelten. Eines der Hauptprobleme des Datenschutzes ist, dass die datenverarbeitenden Unternehmen oft außerhalb der EU ansässig sind bzw. die Daten der Nutzerinnen und Nutzer auf Servern außerhalb der EU verarbeitet werden. Es wird deutlich, dass für einen effektiven Datenschutz Regelungen unerlässlich sind, die keine nationalen Grenzen kennen. Der Grundrechtsschutz kann nicht an Grenzen Halt machen, die das Netz nicht hat.

Eine starke europäische Datenschutz-Grundverordnung

Wir brauchen Regelungen, nach denen sich die Anbieter an die Gesetze des Landes halten müssen, in denen die Nutzerinnen und Nutzer sind – dieses so genannte **Marktortprinzip** muss zur Geltung kommen. Dieses ist im Entwurf einer DS-GVO vorgesehen, was wir ausdrücklich begrüßen.

Am **Einwilligungsvorbehalt** darf nicht gerüttelt werden. Verbraucherinnen und Verbraucher müssen freiwillig und informiert entscheiden können, ob sie in die Verarbeitung ihrer personenbezogenen Daten einwilligen. Immer wieder verstecken sich Einwilligungserklärungen in langen und unleserlichen Nutzungsbedingungen, die häufig nur begrenzt über die verarbeiteten Daten und die Art der Verarbeitung informieren. Verbraucherinnen und Verbraucher haben daher häufig keine Kenntnis, dass sie bereits durch das Surfen auf einer Internetseite einer Datenverarbeitung zustimmen. Auch sind sie im Dunkeln darüber, welche Daten zu welchen Zwecken verarbeitet werden. In anderen Fällen ist die Einwilligung – beispielsweise in einem gesetzten Häkchen – voreingestellt und muss aktiv entfernt werden (opt-out). Daneben gibt es Angebote und Dienstleistungen im Internet, die für Verbraucherinnen und Verbraucher überhaupt nur dann nutzbar sind, wenn sie in die Verarbeitung ihrer Daten zu Werbezwecken oder deren Übermittlung an Dritte einwilligen. Eine in solchen – gekoppelten - Fällen erteilte Einwilligung der Verbraucherinnen und Verbraucher ist jedoch niemals freiwillig.

Die **Zielvorgaben** des Datenschutzes, **Datensparsamkeit, Datenvermeidung** und die **Zweckbindung jeglichen Umgangs mit Daten** müssen gesetzlich stärker verankert werden. Insbesondere bei der Zweckbindung von Daten müssen gesetzliche Grenzen das erlaubte Maß an Zweckänderungen eindeutig abstecken. Verstöße dagegen müssen konsequenter verfolgt und geahndet werden. Wir wollen, dass die Bürgerinnen und Bürger jederzeit ihre grundlegenden Datenschutzrechte kennen können.

Wir wollen ein uneingeschränktes **Recht auf Datenportabilität** für Verbraucherinnen und Verbraucher, die Internetdienste nutzen. Durch die Schwierigkeit, Daten, die einmal bei Anbietern bzw. in bestimmten Plattformen liegen, zu exportieren, entstehen derzeit Lock-In-Effekte: Verbraucherinnen und Verbrauchern wird der vertraglich mögliche Wechsel zu einem anderen Anbieter in vielen Fällen unnötig erschwert. Von einem Recht auf Datenportabilität sollte umfasst sein, dass Verbraucherinnen und Verbraucher ihre einmal auf einer Plattform abgelegten oder eingestellten Daten barrierefrei zu einer anderen Plattform „transportieren“ dürfen oder eine elektronische Kopie ihrer Daten erhalten müssen. Dadurch werden die Kontrolle der Verbraucherinnen und Verbraucher über ihre Onlinedaten und überdies der Wettbewerb zwischen den Unternehmen gestärkt.

Wir brauchen Regelungen, die den besonderen Anforderungen beim **Schutz personenbezogener Daten von Kindern und Jugendlichen** gerecht werden.

Nur **starke, unabhängige und gut ausgestattete Aufsichtsbehörden**, die spürbar hohe Bußgelder verhängen können, sind in der Lage Verstöße zu verhindern, aufzudecken und Ordnungswidrigkeiten und Straftaten im Datenschutzrecht effektiv zu ahnden. Solange die Strafen der Höhe nach nur einen Bruchteil des „Ertrages“ darstellen, den verantwortliche Stellen durch mangelnden Datenschutz „erwirtschaften“ (dieser kann von Einsparungen durch nicht getätigte Investitionen in den Datenschutz bis hinzu Erträgen aus entsprechend kalkulierter Kriminalität reichen) und die Aufsichtsbehörden nicht genügend Personal und Mittel zur Verfügung haben, gibt es einen finanziellen Anreiz für unlautere Geschäftspraktiken. Wir wollen, dass die Aufsichtsbehörden in Europa gut zusammenarbeiten und so eine **konsistente Anwendung des Datenschutzes in allen Mitgliedstaaten** gewährleisten. Wir sprechen uns aber deutlich gegen den Vorschlag der

Europäischen Kommission in ihrem Entwurf einer Datenschutz-Grundverordnung (DS-GVO) aus, dass diese selbst in verschiedenen Fragen als eine Art Suprabehörde das letzte Wort bei der Auslegung der Verordnung hat. Diese Aufgabe muss zwingend bei den unabhängigen Aufsichtsbehörden verbleiben und darf nicht in ein politisches Gremium verlagert werden.

Privacy by design und Privacy by default

Nahezu alle Herausforderungen, vor denen der Datenschutz heute steht, machen deutlich, dass ein rein reaktives Datenschutzrecht nicht ausreicht, um die Grundrechte der Verbraucherinnen und Verbraucher zu gewährleisten.

Eröffnen Verbraucherinnen und Verbraucher beispielsweise einen Account bei einem Sozialen Netzwerk oder nehmen sie ein neu erworbenes Smartphone in Betrieb, so müssen sie sich durch teils sehr umständliche und breit gefächerte Einstellungsebenen kämpfen, bis sie überhaupt wissen, welche Daten öffentlich zugänglich sind, ob Daten in der Cloud gespeichert werden oder welche Dienste auf die GPS Funktion oder das Adressbuch ihres Telefons zugreifen. Die Voreinstellungen sind hier in der Regel eben so datenschutzunfreundlich wie undurchsichtig.

Wir wollen, dass Verbraucherinnen und Verbraucher bei der Nutzung neuer Techniken oder Dienste zu jeder Zeit volle Kontrolle darüber haben, welche Daten erhoben, verarbeitet oder veröffentlicht werden. Wir fordern daher, den Grundsatz ***„Privacy by default“*** *gesetzlich zu verankern. Damit wären alle Dienste oder Endgeräte verpflichtend so datenschutzfreundlich wie möglich voreinzustellen. Es muss den Verbraucherinnen und Verbrauchern überlassen bleiben, und durch einfache bzw. plakative Benutzerführung auch faktisch möglich sein, Apps oder Diensten den Zugriff auf einzelne Daten zu gewähren oder einzelne Daten zur Speicherung in der Cloud freizugeben.*

Router, intelligente Stromzähler oder Smartphones aber auch Dienstleistungen im Internet wie Suchmaschinen führen zu massenweiser Verarbeitung personenbezogener Daten. Es ist weder zielführend noch ökonomisch sinnvoll, wenn Datenschutzprobleme erst bei der Verwendung von Daten beobachtet werden und durch nachträgliche Änderungen oder Nachrüstungen auf diese reagiert werden muss. Zum einen hat die persönlichkeitsrelevante Datenverarbeitung dann bereits stattgefunden, zum anderen können nachträgliche Korrekturen sehr zeit- und kostenintensiv sein. Nützlich ist ein Konzept, das bereits bei der Herstellung von Endgeräten oder der Programmierung von Anwendungen ansetzt und den Datenschutz über den gesamten Lebenszyklus einer Technologie hinweg – von der Herstellung über die Nutzung bis hin zur Entsorgung - von vornherein mitdenkt.

Wir brauchen einen präventiven Ansatz, um etwaige Gefahren für Datenschutz schon bei der Entwicklung einer neuen Technik festzustellen. Der Grundsatz ***„Privacy by Design“*** *muss gesetzlich geregelt, ggf. durch Produkthaftungsregelungen flankiert und Forschung hierzu befördert werden.*

Digitale Geldbörse - Online und mobile Payment

Finanztransaktionen finden immer häufiger über digitale Infrastrukturen statt. Dies nicht nur im Bereich des Onlinebanking und der Online-Bezahldienste, sondern auch beim alltäglichen Einkaufen im Geschäft. Wenn Verbraucherinnen und Verbraucher an der Kasse mit ihrer Kreditkarte oder per Lastschrifteinzugsverfahren bezahlen, finden internetbasierte Datenverarbeitungen statt. Erste Techniken des mobilen Bezahlens via Smartphone stecken bereits in den Startlöchern. Sowohl Internetzahlungsdienste als auch Techniken für mobiles Bezahlen müssen so gestaltet werden, dass Verbraucherinnen und Verbraucher keine Angst vor Betrug im Zahlungsverkehr oder Missbrauch ihrer Zahlungsdaten haben müssen. Der Erfolg von online und mobile Payment-Diensten hängt entscheidend vom Vertrauen der Verbraucherinnen und Verbraucher in die neuen Techniken und Möglichkeiten ab.

Alle Bezahlformen des Online und mobile Payment erfordern Sicherheitssysteme auf hohem Niveau unter Gewährleistung der Nutzbarkeit. Anbieter sollten IT-Sicherheit stärker in den Produkten implementieren. Dies kann über gesetzliche Anreize wie beispielsweise durch Produkthaftungsregelungen oder eine Beweislastregelung befördert werden. Darüber hinaus sollten Anbieter verpflichtet werden, Nutzer im Fall von Datenlecks unmittelbar zu informieren und Sicherheitslücken unverzüglich zu schließen. Auch dies könnte durch Produkthaftungsregelungen befördert werden.

Onlinebanking und Online-Bezahlsysteme

Bei der Nutzung von Onlinebanking und Online-Bezahlsystemen müssen Verbraucherinnen und Verbraucher darauf vertrauen können, dass sie und ihr Vermögen vor unberechtigtem Zugriff geschützt sind. Bevor eine Zahlung online veranlasst werden kann, muss durch starke Authentifizierungsmechanismen die Berechtigung des Nutzers oder der Nutzerin sichergestellt sein.

Um dies zu erreichen sollten Anbieter von Zahlungsdiensten verschlüsselte Verfahren nutzen und die Anzahl der möglichen Anmeldeversuche, die Sitzungszeit und die Gültigkeitsdauer von Passwörtern begrenzen. Flankierend sollten sie Beratungsangebote für Verbraucherinnen und Verbraucher anbieten, welche Selbstschutzmaßnahmen diese ergreifen können.

Derzeit geht der Trend im Internet dahin, dass sowohl Händler als auch Verbraucherinnen und Verbraucher beim selben Zahlungsdienstleister angemeldet sein müssen. Dies führt nicht nur dazu, dass Verbraucherinnen und Verbraucher gezwungen werden, ihre Kontodaten bei etlichen Diensten zu hinterlegen und Händler über etliche dieser Dienste Zahlungen abzuwickeln, es schränkt zudem auch den Wettbewerb unter den Zahlungsdienstleistern ein. Verbraucherinnen und Verbraucher sollten ihren

Zahlungsdienstleister frei wählen können. Wenn sie sich bei einer Vielzahl von Zahlungsdienstleistern registrieren müssten, geht ihnen der notwendige Überblick über erfolgte Transaktionen und ggf. auch missbräuchliche Abbuchungen abhanden.

*Neue Online-Bezahlformen sollten daher auf **standardisierten Verfahren** aufsetzen, so dass Verbraucherinnen und Verbraucher ggf. einen anderen Zahlungsdienstleister als den des Händlers nutzen können. Nur durch eine freie Wahl des Zahlungsdienstleisters kann dauerhaft ein **funktionierender Preis- und Leistungswettbewerb** ermöglicht werden.*

mobile Payment

Mobiltelefone sind fast ständig online erreichbar und dadurch auch besonders angreifbar. Sicherheitssoftware hat sich, anders als beim PC, noch nicht durchgesetzt. So kann Schad- oder Spionagesoftware beispielsweise über Apps oder Updates anderer Anwendungen in das Smartphone gelangen. Auch wird es durch die immer mehr werdenden Anwendungen, die zu Marketingzwecken Zugriff auf Daten verlangen, angreifbar.

Verschiedenste Formen des Bezahlens werden derzeit entwickelt und erprobt. Auch beim kontaktlosen Bezahlen müssen besondere Sicherheitsanforderungen erfüllt werden, insbesondere muss der Nutzer die Kontrolle über sein mobiles Portemonnaie behalten. Welcher Betrag mit welchem Mittel bezahlt wird, muss vom Nutzer jeweils aktiv zu bestätigen sein. Keinesfalls dürfen Abbuchungen über Near-Field-Technologien von den Verbraucherinnen und Verbrauchern unbemerkt von statten gehen.

Die heute bestehenden hohen Sicherheitsstandards beim Online-Banking und bei Online-Zahlungen dürfen beim Mobile Payment keinesfalls unterschritten werden (Zwei-Wege-Autorisierung). Der Wettbewerb der Anbieter darf keinen Anlass bieten, Umgehungen zu programmieren, bei denen die Sicherheit und der Datenschutz zu Gunsten einer kostengünstigeren Bezahlmöglichkeit vermindert werden.

Marktwächter digitale Welt

Die digitale Welt zeichnet sich dadurch aus, dass der technologische Fortschritt ständig neue Marktsegmente und -teilnehmer hervorbringt. Zudem bietet der digitale Markt im Vergleich zu anderen Märkten viele scheinbar „kostenfreie“ Angebote, was ihn deutlich von anderen Märkten unterscheidet. Verbraucherinnen und Verbraucher haben es schwer, seriöse von unseriösen Angeboten zu unterscheiden. Analoge Strukturen und Zuständigkeiten verhindern in der Regel sowohl eine umfassende zivilgesellschaftliche Marktbeobachtung wie auch staatliche Marktmissbrauchsaufsicht.

Wir brauchen daher einen Marktwächter in der digitalen Welt, der die Marktstrukturen beobachtet, Beschwerden von Verbraucherinnen und Verbrauchern sammelt und systematisch auswertet, Missstände an die zuständigen Aufsichtsbehörden meldet und im Zweifel auch die Rechte der Verbraucherinnen und Verbraucher durchsetzt. Darüber hinaus soll der Marktwächter in der Verbraucherbildung aktiv sein.

Der Marktwächter digitale Welt soll nicht nur konkrete Beschwerden aufnehmen, bündeln und überprüfen, ob eine systematische Benachteiligung der Verbraucherinnen und Verbraucher vorliegt, sondern auch AGB sowie verbraucherschützende Vorschriften (bspw. Button-Lösung) im Online-Handel kontrollieren. Die Überwachung der datenschutzrechtlichen Vorschriften sowie des Umgangs mit Daten im digitalen Bereich von der online-Plattform bis hin zu Praktiken in Ladengeschäften bspw. mit RFID Chips, gehören ebenso zu seinen Aufgaben. Er sammelt Verbraucherbeschwerden und wertet diese systematisch aus. Kurz: Er soll den digitalen Markt **beobachten**.

Die Marktbeobachtung soll Missstände evident und öffentlich machen, wo heute auf Grund mangelnder Ressourcen und Erkenntnisse Missstände nur „gefühlt“ sind.

Zu seinen Aufgaben soll es auch zählen, Verbraucherinnen und Verbraucher zu **beraten**. So können die aus der Marktbeobachtung gewonnenen Kenntnisse dazu genutzt werden, auf einer Internetseite gängige verbraucherfeindliche AGB vorzustellen oder Ergebnisse eines Datenschutzbestimmungs-Checks zu veröffentlichen, um Vergleichsmöglichkeiten für Verbraucherinnen und Verbraucher zu schaffen.

Der Marktwächter soll für **Klarheit und Wahrheit auf dem Markt** sorgen, Transparenz über Angebote im Internet schaffen, die Entwicklung von Best Practice Modellen insbesondere im Bereich verallgemeinerter AGB oder Datenschutzbedingungen fördern und Optionen zum Umgang mit Daten aufzeigen.

Der Marktwächter soll systematische Benachteiligung von Verbraucherinnen und Verbrauchern **bekämpfen**. Er soll Missstände und unseriöse Angebote bei der zuständigen Aufsichtsbehörde anzeigen. Im Unterlassungsklagegesetz (UKlaG) muss im Zuge der Einführung eines Marktwächters für die digitale Welt klargestellt werden, dass Datenschutzvorschriften, soweit sie Verbraucherrechte betreffen, Verbraucherschutzgesetze im Sinne des UKlaG sind.

Modernes Urheberrecht schützt auch Verbraucher

Die SPD steht für ein modernes Urheberrecht, das den Anforderungen der digitalen Welt Rechnung trägt. Das Motto lautet: „Vergüten statt verbieten“: Für das Einkommen von Kultur- und Kreativschaffenden ist das Urheberrecht von zentraler Bedeutung. Auch im digitalen Zeitalter muss aus der Verwertung geistigen Eigentums eine angemessene Vergütung erwachsen. Auf der anderen Seite muss die reale Nutzung des Netzes zur legalen Nutzung werden. Hierzu müssen moderne – für Urheber und Nutzer gleichermaßen attraktive – Online-Angebote und Geschäftsmodelle für das Internet etabliert und der Trend zur Nutzung legaler Online-Angebote unterstützen werden. Eine Kulturflatrate lehnen wir ab.

Es bedarf neuer Geschäftsmodelle und Vermarktungsstrategien, die sowohl die Rechte der Urheber wahren als auch die digitalen Realitäten und Gewohnheiten der Verbraucherinnen und Verbraucher berücksichtigen. Die derzeitige Situation, in der Verbraucherinnen und Verbraucher auf Grund veränderter gesellschaftlicher Rahmenbedingungen mit dem Urheberrecht in Konflikt geraten, ist genauso wenig haltbar, wie daraus resultierende Einnahmeverluste für Urheberinnen und Urheber.

Diese neuen Geschäftsmodelle und Vermarktungsstrategien sollen sowohl den Urheberinnen und Urhebern und Verwerterinnen und Verwertern von Rechten dienen, als auch zugleich eine einfache und verbraucherfreundliche legale Nutzung geschützter Inhalte ermöglichen, was auch den Nutzerinnen und Nutzern die nötige Rechtssicherheit bietet. Die Entwicklung legaler kommerzieller Geschäftsmodelle sollte daher unterstützt und vorangetrieben werden.

Bei der notwendigen Reform des Urheberrechts müssen aus verbraucherpolitischer Sicht folgende Nutzerinteressen berücksichtigt werden:

Weiterveräußerung digitaler Werke

Der EuGH hat 2012 in einem Vorabentscheidungsverfahren (Az.: C-128/11) entschieden, dass Softwarehersteller den Weiterverkauf „gebrauchter“ Lizenzen nicht untersagen dürfen, wenn der Käufer diese per Download erworben hat und ihm dabei ein zeitlich unbegrenztes Nutzungsrecht eingeräumt wurde. Körperliche Kopien auf CDs und ähnlichen Datenträgern seien insofern aus dem Internet heruntergeladenen Programmkopien gleichzustellen. Allerdings müsse der Erwerber beim Weiterverkauf die Kopie von seinem eigenen Rechner löschen. Es ist zu prüfen, ob und inwiefern die Grundsätze dieser Entscheidung zu UsedSoft auch auf den Bereich des Handels mit digitalen Mediengütern (beispielsweise Filme, Musik, eBooks) übertragen werden können.

Es ist derzeit unklar, ob auch der Kauf und Weiterverkauf von Mediendateien, also etwa von Filmen und Musikstücken, in diesem Sinne beurteilt werden muss. Das Urteil findet auf solche Fälle keine unmittelbare Anwendung. Die Urteilsbegründung legt eine Übertragbarkeit

jedoch nahe, insofern sie auf eine parallele Anwendung des sogenannten Erschöpfungsgrundsatzes abhebt. Im Verständnis der Verbraucherinnen und Verbraucher handelt es sich in der Regel um einen Kaufakt, wenn sie ein eBook, eine Musikdatei oder einen Film herunterladen. Es bleibt daher aus Sicht der Verbraucherinnen und Verbraucher unklar, warum digitale Werkexemplare im Gegensatz zu Datenträgern nicht weiterverkauft werden dürfen. Es ist daher zu prüfen, wie der Weiterverkauf von digitalen Gütern rechtlich ermöglicht werden kann.

Privatkopien

Angesichts der zunehmenden Bedeutung von technischen Zugangskontrollen ist die Technikfestigkeit der Schrankenbestimmungen dahingehend zu prüfen, ob und wie sichergestellt werden kann, dass die Schranken nicht leer laufen. Auch in der digitalen Welt muss die Möglichkeit einer digitalen Privatkopie erhalten bleiben.

Die Entscheidung, welche Nutzungen im Urheberrecht durch Schrankenregelungen privilegiert sind, muss auch im digitalen Raum beim Gesetzgeber verbleiben. Der Einsatz technischer Schutzmaßnahmen sowie die Praxis, den Umfang privaten Kopierens in AGB zu bestimmen, verlagert diese Definitionsmacht auf die Unternehmen. Die Privatkopie und andere Schrankenbestimmungen sind jedoch Teil eines Gesellschaftsvertrags, dessen Inhalt nicht im privaten Geschäftsverkehr zur Disposition gestellt werden sollte.

Abmahnungen begrenzen

Abmahnungen gegen potentielle Rechtsverletzer sind ein legitimes und wichtiges Instrument der Rechtsverfolgung, Zunehmend werden Verbraucherinnen und Verbraucher aber mit einer neuartigen „Abmahnindustrie“ konfrontiert, die das Instrument missbraucht, um mit der Abmahnung Gewinne zu erzielen, die mit einer normalen Lizensierung nicht zu erzielen wären. Dabei wird die Abmahnung selbst zum „Geschäftsmodell“.

Die Rechtsverfolgung der Rechteinhaber darf sich aber nicht einseitig auf Verbraucherinnen und Verbraucher konzentrieren. Inzwischen haben in Deutschland etwa 4,3 Mio. Menschen eine Abmahnung wegen angeblicher Urheberrechtsverletzung erhalten. Massenabmahnungen sind für eine kleine Gruppe von spezialisierten Anwaltskanzleien ein lukratives Geschäftsmodell geworden. Dem muss entgegengewirkt werden. Familien dürfen nicht mit überzogenen Gebühren von durchschnittlich 700 bis 800 Euro, mitunter auch deutlich darüber, belastet werden, wenn ein Kind einen Song ins Internet gestellt hat oder ein Dritter über einen vermeintlich nicht ausreichend gesicherten Internetanschluss unbefugt Dateien hochgeladen hat. Aus der Abmahnung gegenüber Privaten darf kein „Geschäft“ werden. Deshalb müssen die Abmahnkosten bei Urheberrechtsverstößen im privaten

Bereich wirksam begrenzt werden. Hierzu brauchen wir eine Streitwertobergrenze für Urheberrechtsverletzungen im privaten Bereich, Korrekturen bei der Beweislastverteilung und einen Gegenkostenanspruch des zu Unrecht Abgemahnten. Wir setzen uns zudem für die Einschränkung des „fliegenden Gerichtsstands“ bei Urheberrechtsverstößen im Internet ein.

Diese gesetzliche Regelung muss so klar gefasst werden, dass keine Zweifel mehr darüber bestehen, in welchen Fällen die Deckelung greift. Insbesondere sind daher Ausnahmetatbestände mit unbestimmten Rechtsbegriffen, die Rechtsunsicherheit schaffen, abzulehnen.