AK – Prinz Eugen-Strasse 20-22, 1040 Vienna

Überarbeitung der Richtlinie zum elektronischen Geschäftsverkehr – Künftiger Digital Service Act

Sehr geehrte Frau Exekutiv-Vizepräsidentin Vestager!

Die Absicherung und die Weiterentwicklung des sektorspezifischen Verbraucherschutzniveaus in Europa ist der Bundesarbeitskammer (BAK) ein besonderes Anliegen. Wir setzen uns mit besonderem Nachdruck dafür ein, dass die **Bedürfnisse der KonsumentInnen an einem zeitgemäßen Schutz vor Intransparenz, Irreführung, Übervorteilung und Betrug im Internet** ausreichend berücksichtigt werden. Wir nehmen daher die Vorarbeiten zur Überarbeitung der RL 2000/31/EG mit dem Ziel eines neuen „Digital Service Act" zum Anlass, Sie um Unterstützung folgender Anliegen zu ersuchen:

Auf allen Plattformen Transparenz der Rankings

Das gibt es bereits:

Transparenzvorschriften für Rankings (ihre Parameter und Gewichtung) gibt es für sogenannte Online-Marktplätze, die der Abwicklung von Onlinekäufen dienen (Revision der RL über unlautere Geschäftspraktiken 2005/29 EG) und Suchmaschinen (VO Transparenz für gewerbliche Nutzer „platform-to-business" 2019/1150 EG).

Das fehlt:

Keine Abhilfe gegen intransparente, algorithmische Reihung von Inhalten gibt es bei Plattformen, die im weitesten Sinn **nutzergenerierte oder von Drittanbietern bereitgestellte (Medien-)Inhalte** bereitstellen. Egal ob YouTube, Facebook, Alexa oder Netflix u.v.m.- für die NutzerInnen erhellt sich nicht, nach welchen Regeln Inhalte ausgespielt werden.

Gerade bei nachrichtenrelevanten Inhalten (wie Newsfeeds), über die sich mittlerweile viele KonsumentInnen vorrangig informieren, darf Klarheit über die angewandten Faktoren der Reihung erwartet werden. Transparenz als Mittel gegen die Manipulation der Meinungsbildung einzusetzen, ist auch demokratiepolitisch äußerst wichtig. Zudem verlangt es die Fairness gegenüber herkömmlichen Medienanbietern, die ihre „Blattlinie" offenlegen.

Onlinewerbung endlich einheitlich regulieren

Das gibt es bereits:

Die e-Commerce Richtlinie enthält in Bezug auf Werbung einige dem klassischen Medienrecht entlehnte Grundsätze. Ihre Beachtung ist weiterhin elementar wichtig für KonsumentInnen. Sie reichen aber bei weitem nicht aus, um zeitgemäß vor Manipulation, Belästigung und Irreführung zu schützen. Die Richtlinie verpflichtet Dienste der Informationsgesellschaft dem Trennungsgrundsatz zwischen Werbung und redaktionellen Inhalten entsprechend zur Kennzeichnung von kommerzieller Kommunikation. Wer Auftraggeber der Werbung ist, muss auch klar hervorgehen. Schließlich müssen die Mitgliedstaaten „Robinson-Listen" jenen KonsumentInnen anbieten, die keine Werbung erhalten

möchten. Diese Maßnahme ist im Ansatz richtig und wichtig, in der Praxis aber nahezu totes Recht geblieben.

Bloß für audiovisuelle Medienanbieter gibt es detailliertere Werbevorschriften (AVMD RL 2018/1808/EG). Mit der jüngsten Richtlinien-Überarbeitung werden Plattformen wie YouTube in den Anwendungsbereich einbezogen. Plattformen, die nicht dominant audiovisuellen Content enthalten, sind nicht erfasst.

Das fehlt:

Die zuvor genannten Werbegrundsätze (Kennzeichnung, Trennung, Offenlegung des Auftraggebers, Beachtung eines zentral verwalteten, generellen Opt-Outs in Bezug auf Werbung) werden systematisch gebrochen, denn effiziente Kontrolle und spürbare Sanktionen fehlen fast vollständig. KonsumentInnen sind nicht nur Intransparenz, Manipulation, Belästigung und rechtswidrigen Werbeinhalten ausgesetzt. Traditionelle Medien, die sich an Werberegeln halten, werden durch unlautere Online-Werbeformen bzw -inhalte grob benachteiligt. **Strikte Aufsicht und Sanktionen gegenüber Verstößen** müssen daher ein wichtiger Eckpunkt der Überarbeitung der Richtlinie sein.

Um dem Selbstbestimmungsrecht von InternetnutzerInnen wirklich gerecht zu werden, müsste die **Robinson-Liste für e-Mailwerbung zu einem echten „Stop-Tracking"-Tool für jede Form der Onlinewerbung** werden. Eine zentral verwaltete Opt-Out-Möglichkeit ist derzeit nur für unangeforderte Mailwerbung einzurichten – Spam ist allerdings nach anderen RL ohnehin untersagt und für unangeforderte Mailwerbung gilt in vielen Mitgliedstaaten ein Opt-In (Zustimmung des Konsumenten). Wer Onlinewerbung insgesamt nicht schätzt, sondern als Belästigung empfindet, hat derzeit keine vertretbaren Möglichkeiten, diese Haltung einfach und wirksam zum Ausdruck zu bringen. An aufgezwungener Werbung verdienen Intermediäre aus der Onlinewerbewirtschaft. Sie verfehlt aber bei nicht werbeaffinen InternetnutzerInnen komplett die Ziele der Auftraggeber.

Derzeit müssen sich KonsumentInnen bei jedem Dienst in unzumutbarer Weise von neuem mit ellenlangen Erklärungen, diffizilen Einstellungen und enormen datenschutz- und medienrechtlichen Umsetzungsdefiziten herumquälen.

Wer nicht will, dass seine digitalen Spuren für Werbezwecke quer durchs Internet verfolgt werden, um individuelle Verhaltensprofile zu erstellen und ebensolche Werbung auszuspielen, sollte sich in eine zentrale Liste eintragen können. Alle Onlinedienste, die ihre Angebote auf das Wohnsitzland der in die Liste eingetragenen Personen ausrichten, haben den Wunsch zu beachten.

Es ist im Übrigen hoch an der Zeit für **ein einheitliches striktes Regulierungsniveau von Onlinewerbung** unabhängig davon auf welchen Seiten die Werbung ausgespielt wird. Bisher gibt es nur ein paar Detailregeln für Werbung in audiovisuellen Medien. Für KonsumentInnen ist es völlig egal, auf welcher Website oder App sie sich aufhalten. Sie haben stets das selben Bedürfnis, vor intransparenter, aggressiver, Gesundheit, Umwelt oder die Jugend beeinträchtigender Werbung usw geschützt zu werden.

Da **Werbung für unseriöse oder betrügerische Dienste** über Hand nimmt, müssen die **Verantwortung in der Kette Werbedienstleister und Plattformen** unbedingt geklärt werden. Da Plattformen über Verhaltensprofile ihrer Nutzer und eine Beteiligung an den Werbeerlösen in die Vermarktungspraktiken von Onlinewerbung involviert sind, sollten sie bezüglich rechtswidriger Werbung stark in die Pflicht genommen werden. Sie sollten **Tools zur eindeutigen Kennzeichnung** von Werbung und dessen Auftraggeber anbieten, die von Werbenden zwingend genutzt werden müssen. Außerdem sollten sie **Werbung auf offensichtliche Rechtswidrigkeiten** hin (zB Fakeshops, verbotene vor allem raubkopierte Waren, Datenklau und Verbreitung von Schadsoftware usw) vorab **automatisiert kontrollieren** müssen. Im Gegensatz zu sonstigen Inhalten besteht bei Werbeinhalten kaum die Gefahr, dass durch automatisierte Filter grundrechtlich geschützte Informations- und Persönlichkeitsrechte verletzt werden.

Sonstige **Webseiten mit Drittanbieterwerbung** (wie Affiliate Marketing) müssen zumindest einen **Beschwerdemechanismus** aufbauen, damit Hinweise auf Werbeverstöße bei den dahinterstehenden Werbe-Intermediären rasch ankommen.

Die **Online-Werbewirtschaft, die Werbung auf Webseiten platziert, haftet** für die rasche Herstellung eines rechtmäßigen Zustandes (Änderung oder Bann der inkriminierten Werbung).

Aufsicht und Sanktionen sind so zu gestalten, dass die enormen, systematischen Vollzugsdefizite beseitigt werden.

KonsumentInnen sollten auch in den Genuss des Schutzes der „platform to business“-VO kommen

Das gibt es bereits:

Diese EU-VO schützt nur Drittanbieter auf Online-Marktplätzen vor Intransparenz und Benachteiligung.

Das fehlt:

Etliche Schutznormen sind auch für KonsumentInnen sinnvoll: zB **Offenlegung von Sperrgründen** auf Plattformen für private Bewertungen, mit usergenerierten Inhalten bzw. Kommentierungsfunktion (Art 3/1c und Art 4). Die Erklärung, wie sich eine **differenzierte Behandlung** von eigenen Waren und jenen von Mitbewerbern auswirkt (Art 7), ist auch gegenüber KonsumentInnen offenzulegen. Auch **Art und Umfang des Datenzugangs** des Vermittlungsdienstes und von Drittanbietern (Art 9) sollte Verbrauchern von der Plattform verständlich erklärt werden. Derzeit gibt es erhebliche Defizite, zB bei den Appstores oder Drittanbieteranwendungen bei Sprachassistenten wie Alexa oder Siri, die nur auf die Datenschutzerklärungen der jeweiligen Entwickler verweisen. Plattformen verpflichten Entwickler vertraglich ohnehin zur Einhaltung von Gesetzen, also auch in Bezug auf Datenschutz und Datensicherheit. Sie sollten KonsumentInnen darüber informieren, welche Kundendaten Plattform und Entwickler miteinander teilen und welche vertraglichen Pflichten sie auf welche Weise kontrollieren. Bei Verstößen haftet die Plattform gemeinsam mit dem Entwickler.

Netzneutralität auf Plattformebene sicherstellen

Das gibt es bereits:

Internetbetreiber sind zur Beachtung von Netzneutralität verpflichtet (Telekom Single Market VO 2015/2120 EG). Netzneutralität bedeutet, dass grundsätzlich alle Daten bei der Übertragung innerhalb von Netzen gleichbehandelt werden. Videos und E-Mails werden gleich schnell durch das Netz bis zum Nutzer transportiert wie Webseiten, Internet-Telefonate und Online-Banking. Netzneutralität bedeutet auch, dass Angebote eines bestimmten Unternehmens nicht bevorzugt werden, dass also etwa nur ein bestimmter Videodienst beschleunigt übertragen wird.

Das fehlt:

Auch **Plattformen mit Torwächterfunktion** brauchen die Vorgabe, sich dem Prinzip der **Netzneutralität** gemäß zu verhalten. Eine Aufsichtsbehörde muss die Einhaltung Plattformen gegenüber kontrollieren. So bedarf es etwa einer Kontrolle, nach welchen Regeln Content Delivery Plattformen Inhalte ausspielen oder Sprachassistenten auf Befehle reagieren. Ziel sollte es sein, Transparenz, Wahlfreiheit und Vielfalt für Verbraucher sicherzustellen.

Bekämpfung von Cybercrime auf Plattformen

Das fehlt:

Cybercrime auf Plattformen (Daten- und Identitätsdiebstahl, Fakeshops, Vorauszahlungsbetrug usw) nimmt stark zu. Dies führt zu erheblichen Vertrauensverlusten auf Seiten der Konsumentinnen in Bezug auf die gefahrlose Nutzung von Onlinediensten generell. In Zusammenarbeit mit den zur Bekämpfung von Internetkriminalität zuständigen Strafbehörden sind u.a. Verhaltensregeln für Plattformen zu entwickeln, die einer Schädigung von Verbrauchern wirksam vorbeugen.

Dazu zählt u.a. die verpflichtende Einführung eines **europäischen Firmenbuchs für Onlineanbieter**. Wesentlich ist aber auch eine **Verpflichtung der Plattformanbieter**,

- die Identität kommerzieller Drittanbieter anhand des Firmenbuchs zu klären.
- eine Versicherung abzuschließen, um KonsumentInnen entschädigen zu können, wenn unseriöse Drittanbieter auf der Plattform nicht greifbar sind oder sich sonst ihrer Verantwortung entziehen.
- Bei sonstiger Sanktion zu verhindern, dass gemeldete rechtswidrige Angebote erneut aufscheinen.
- zu unverzüglicher Prüfung der von KonsumentInnen gemeldeten Betrugsfälle.

Abgestufte Haftung der Internetbetreiber beibehalten

Das gibt es bereits:

Die Maxime, Internetzugangs- und Hostanbietern keine allgemeinen, pauschalen Vorabprüfpflichten bei Sachverhalten aufzuerlegen, die Grundrechte berühren, ist weiterhin beizubehalten (Art 15 e-Commerce RL). Bei Abwägung der Für und Wider präventiver Filtermaßnahmen überwiegen die Bedenken bezüglich damit einhergehender Beschränkungen der Grund- und Freiheitsrechte nach der EMRK bei weitem. Der Anwendungsbereich für „proaktive Maßnahmen“ (im Wesentlichen einer Algorithmenkontrolle), wie sie die VO über die Bekämpfung terroristischer Onlineinhalte enthält, sollte keinesfalls durch weitere spezifische Derogationen von Art 15 ausgedehnt werden.

Genaue Regeln für „notice and take down“

Das gibt es bereits:

Die e-Commerce RL enthält bereits ein sogenanntes „Notice und Takedown“-Verfahren. Internetbetreiber können von einer Haftungsbefreiung profitieren, wenn sie den Zugang zu Informationen schnellstmöglich entfernen oder sperren, sobald sie Kenntnis von deren rechtswidrigem Charakter erlangen. Die Regeln gelten für jegliche Art von illegalen oder rechtswidrigen Inhalten. Dienste Anbieter fungieren dabei aber nicht als Internetpolizei – sie dürfen jedenfalls nicht zu einer allgemeinen, aktiven Überwachung aller Inhalte gezwungen werden. „Notice und Action“-Mechanismen wirken sich unmittelbar auf die Meinungsfreiheit aus. Derzeit müssen die Zugangs- und Hostbetreiber entscheiden, wann und wie Inhalte aus dem Netz entfernt werden. Dabei müssen sie oft über konkurrierende Rechte und Interessen entscheiden. Da Unternehmen Gerichte bei dieser Aufgabe nicht ersetzen können, ist eine „privatisierte Rechtsdurchsetzung“ abzulehnen.

Das fehlt:

Plattformen, die sich weigern, Inhalte rasch zu löschen, können für diese Inhalte haftbar gemacht werden. Daher neigen sie dazu, unter Druck eher zu viel als zu wenig zu löschen. Die Gefahr des „Overblocking“ der Plattformen wird bei der Umsetzung der Urheberrechte RL sichtbar. Auch das

deutsche Netzwerk-Durchsetzungsgesetz, das Hetze und Fakeinhalte unterbinden soll, steht im Spannungsfeld zwischen rascherer Rechtsdurchsetzung und dem Schutz der Meinungsfreiheit. Sorgfältige grundrechtskonforme Abklärung setzt jedenfalls die Entscheidungsarbeit unabhängiger Stellen voraus. Wesentlich ist, Kriterien für die Zusammensetzung der über Sperren und Löschung entscheidenden Gremien vorzugeben. Damit soll gewährleistet sein, dass nicht die Plattformen selbst entscheiden, sondern Unabhängigkeit, Fachkenntnisse, jährliche Berichtspflichten und Beaufsichtigung durch ein staatliches Organ vorhanden sind.

Wir hoffen, dass unsere Anregungen berücksichtigt werden und stehen für weitere Auskünfte gerne zur Verfügung.

Mit freundlichen Grüßen

Renate Anderl
Präsidentin

Christoph Klein
Direktor