ZWST

care digital

Netzpolitik und Verbraucherschutz

inhalt

Impressum *Stand September 2023*

Herausgeber	Zentralwohlfahrtsstelle der Juden in Deutschland e.V. Hebelstraße 6 60318 Frankfurt am Main T 069 944371 0 E zentrale@zwst.org
Konzept und Redaktion	Laura Cazés, Regina Potomkina, Irina Rosensaft
Gestaltung	DAUBERMANN
Bildnachweise	ZWST (sofern nicht anders angegeben)

Mabat – professionalisierung, innovation und digitalität.

Copyright: Debi Simon

Irina Rosensaft,
Leitung Fachbereich Digitale Transformation

MABAT (Hebr. „Blick“) ist der Fachbereich für Digitale Transformation der ZWST, der durch das Bundesministerium für Familie, Senioren, Frauen und Jugend gefördert wird.

MABAT setzt sich seit 2019 zum Ziel, die Digitalität in der Jüdischen Wohlfahrtspflege auf mehreren Ebenen zu fördern und weiterzuentwickeln: Zielgruppen und Mitglieder sollen zur Teilhabe an gesellschaftlichen Prozessen befähigt werden, und Organisationen dabei unterstützt werden, ihre Arbeitsprozesse und Angebote modern, effizient und zielgruppenorientiert zu gestalten.

Die Vermittlung Digitaler Kompetenzen und Digital Literacy steht auf der Ebene vulnerabler Zielgruppen im Fokus, um die Förderung sozialer und gesellschaftlicher Teilhabe, sowie den Abbau struktureller Barrieren von Kindern und Jugendlichen, Senior:innen und unterstützungsbedürftigen Gruppen sicherzustellen.

Auf der Ebene der Mitgliedsorganisationen unterstützt die ZWST mit MABAT beim Aufbau der Infrastruktur sowie bei der Professionalisierung in Form von Fortbildungen und Trainings für Führungskräfte, Mitarbeitende und Ehrenamtliche.

Ebenso findet auf der Ebene des Spitzenverbandes ein tiefgreifender Prozess der Digitalen Transformation im Rahmen der Organisationsentwicklung statt, der mit einer Steigerung der digitalen Expertise der Mitarbeitenden und der Abteilungen einhergeht. Das kontinuierliche Erlernen neuer digitaler Kompetenzen wird als Aufgabe für den gesamten Verband verstanden und fördert bereichsübergreifende Arbeitsprozesse. Darüber hinaus werden digitale Themen in allen Bereichen projektbezogen und zielgruppengerecht platziert.

Die dreitägige Online-Tagung zum Thema **„Netzpolitik und Verbraucherschutz in digitalen Räumen“** im Mai 2022 hatte zum Ziel, über netzpolitische Regulierungen und Online-Verbraucherschutz aufzuklären, digitale Trends kritisch zu hinterfragen und digitale Teilhabe zu ermöglichen. Insbesondere ging es um die Sichtbarmachung von Expertisen in Bereichen wie Schutz von persönlichen Daten, Regulierung von Online-Plattformen, Kryptowährungen und Künstliche Intelligenz, Cybermobbing, Cyberkriminalität und Jugendschutz.

Mit dem Einsatz digitaler Anwendungen, mit der Verlegung unserer Angebote in digitale Räume eröffnet sich eine neue Ebene, auf der der Schutz für Gemeindemitglieder gewährleistet werden muss. Der richtige Umgang mit Daten, Prozessen und auch der Schutz unserer Netzwerke stellt eine besondere Unsicherheit dar. Deshalb ist auch das Verständnis von Präventions- und Schutzmaßnahmen so elementar für die Arbeit in jüdischen Gemeinden und Organisationen. Diese Broschüre soll den Einstieg in diese komplexe Thematik bieten und jüdischen Organisationen einen Überblick über zentrale Hinweise und niedrigschwellige Maßnahmen liefern.

Bleiben Sie mit uns in Kontakt:
digitalisierung@zwst.org

Der Fachbereich für Digitale Transformation der ZWST wird durch das Bundesministerium für Familie, Senioren, Frauen und Jugend im Rahmen des Förderprogramms „Zukunftssicherung der Freien Wohlfahrtspflege durch Digitalisierung“ unterstützt.

Gefördert vom

Bundesministerium
für Familie, Senioren, Frauen
und Jugend

glossar

Alle QR-Codes aus der Broschüre finden Sie zum Abscannen auf den Seiten 43 bis 46.

BIG DATA
Mit Big Data bezeichnet man größere und komplexere Datensätze, vor allem von neuen Datenquellen. QR-Code 2

CLICK STREAM
Der elektronische Weg, den Nutzer:innen bei der Navigation zwischen Webseiten und ihren Subseiten zurücklegen.
QR-Code 3

IP-ADRESSE
Eine IP-Adresse ist eine numerische Darstellung des Standortes, von dem aus ein Gerät mit dem Internet verbunden ist.
QR-Code 4

VPN
Ein VPN (Virtual Private Network) ist ein Dienst, der eine sichere, verschlüsselte Online-Verbindung herstellt.
QR-Code 5

NETFLIX
Bei Netflix handelt es sich um einen sogenannten Video-on-Demand (dt.: „Video auf Abruf“) Dienst. Auf der Webseite können Sie zahlreiche Filme und Serien legal anschauen. QR-Code 6

PROFILING
Profiling beschreibt die automatisierte Verarbeitung personenbezogener Daten mit dem Ziel der Erstellung eines Profils mit klaren Unterscheidungs- und Abgrenzungsmerkmalen. QR-Code 7

MICROTARGETING
Microtargeting ist eine Marketingform, welche Unternehmen erlaubt, ihre Zielgruppen extrem personalisiert anzusprechen. QR-Code 9

DATA LITERACY
Data Literacy oder
Datenkompetenz beschreibt die Fähigkeit, mit Daten kompetent umzugehen.
QR-Code 10

CHERRY PICKING
Cherry Picking bzw. Rosinenpicken ist ein bildlicher Begriff für das Bemühen, sich von etwas Bestimmtem nur die attraktivsten Teile zu sichern, um die eher unattraktiven anderen zu überlassen.
QR-Code 12

glossar

Alle QR-Codes aus der Broschüre finden Sie zum Abscannen auf den Seiten 43 bis 46.

FILESHARING
Von Filesharing spricht man, wenn Nutzer:innen Dateien über ein Netzwerk miteinander teilen. Dieses ist in den meisten Fällen internetbasiert, wobei sich die Dateien entweder auf den Computern der einzelnen Nutzer:innen oder auf dedizierten Servern befinden, von wo sie an die jeweiligen interessierten User:innen verteilt werden.

QR-Code 13

URHEBERRECHT
Das Urheberrecht umfasst gesetzliche Regelungen zur Verwertung und zum Schutz des geistigen Eigentums. Dabei definiert es die Rechte von Urhebern und Verwertern.
QR-Code 14

HATE SPEECH
Hate Speech kommt aus dem Englischen und bedeutet übersetzt „Hassrede“. In menschenverachtenden Aussagen werden Einzelne oder Gruppen abgewertet. Die sprachlichen Angriffe können auf Merkmale wie Hautfarbe, Herkunft, Sexualität, Geschlecht, Alter, Behinderung oder Religion von Menschen zielen. Rechtsextreme und rechtspopulistische Akteur:innen nutzen dabei auch digitale Räume, um menschenverachtende Einstellungen in der Mitte der Gesellschaft zu verbreiten.
QR-Code 15

FSK
Die Freiwillige Selbstkontrolle der Filmwirtschaft (FSK) ermittelt die Freigaben für Filme mit fünf Alterskennzeichen.
QR-Code 23

USK
Die Unterhaltungssoftware Selbstkontrolle (USK) ist eine freiwillige Einrichtung der Games-Branche. Sie ist zuständig für die Prüfung zur Alterseinstufung von digitalen Spielen in Deutschland.
QR-Code 24

FAKE NEWS
Fake News – wörtlich übersetzt „gefälschte Nachrichten“ – sind Informationen in Form von Texten, Fotos oder Videos, die nicht der Wahrheit entsprechen. Sie sind mit unbewiesenen Behauptungen gespickt und beziehen sich auf nicht geschehene Ereignisse oder Handlungen. Häufig werden sie über elektronische Kanäle, bevorzugt über soziale Medien, verbreitet.
QR-Code 27

SEXTING
Sexting ist ein Kofferwort, bestehend aus den Wörtern „Sex“ und „Texting“. Es beschreibt das Versenden und Empfangen selbstproduzierter, freizügiger Aufnahmen via Computer oder Smartphone.
QR-Code 28

glossar

Alle QR-Codes aus der Broschüre finden Sie zum Abscannen auf den Seiten 43 bis 46.

CYBER GROOMING
Sexuelle Belästigung und sexueller Missbrauch von Kindern und Jugendlichen im Internet geschehen leider regelmäßig. Die Vorbereitung dieser Straftaten nennt man Cybergrooming.
QR-Code 29

CYBER MOBBING
Unter Cyberbullying oder Cybermobbing versteht man die Beleidigung, Bedrohung, Bloßstellung oder Belästigung von Personen mithilfe von Kommunikationsmedien, beispielsweise über Smartphones, E-Mails, Websites, Foren, Chats und Communities.
QR-Code 30

SMART HOME
Unter dem Begriff Smart Home versteht man die intelligente Vernetzung einzelner Komponenten innerhalb eines Hauses, die zentral über Endgeräte gesteuert und überwacht werden.
QR-Code 31

PARENTAL GUIDANCE-REGELUNG
Die sogenannte Parental Guidance-Regelung wurde mit der Überarbeitung des Jugendschutzgesetzes im Jahr 2003 eingeführt. Diese besagt, dass ein Film mit einer Freigabe ab 12 Jahren auch von Kindern ab 6 Jahren geschaut werden kann, wenn diese in Begleitung eines Elternteils sind. Die PG-Regelung lässt sich in § 11 Absatz 2 des Jugendschutzgesetzes finden.
QR-Code 32

SCHADENSERSATZANSPRUCH
Ein Schadensersatzanspruch entsteht unter definierten Bedingungen und verpflichtet dann den Schädiger zum Ausgleich des Schadens gegenüber dem Geschädigten.
Die Voraussetzungen sind, dass der Schädiger rechts- und/oder vertragswidrig gehandelt hat, diese Handlung schuldhaft (fahrlässig oder vorsätzlich) erfolgte und dem Geschädigten daraus ein echter, bezifferbarer Schaden entstanden ist.
QR-Code 33

INVITATIO AD OFFERENDUM
Die invitatio ad offerendum bezeichnet eine rechtlich nicht beachtliche Handlung zur Vertragsanbahnung, d. h. Aufforderung zur Abgabe eines Angebotes.
QR-Code 34

glossar

Alle QR-Codes aus der Broschüre finden Sie zum Abscannen auf den Seiten 43 bis 45.

WIDERRUFSRECHT
Das Widerrufsrecht bezeichnet die innerhalb einer Frist nach Vertragsabschluss mögliche Rücktrittserklärung von Verbraucher:innen und findet bei Kauf- und Versicherungsverträgen, sowie sonstigen Vertragsabschlüssen Anwendung.
QR-Code 35

FERNABSATZGESCHÄFT
Bei dem Fernabsatzgeschäft handelt es sich um eine besondere Form eines Verbrauchervertrages, also um einen Vertrag zwischen einem Verbraucher i.S.d. § 13 BGB [Bürgerliches Gesetzbuch] und einem Unternehmer i.S.d. § 14 BGB. Die Besonderheit liegt darin, dass ein Fernabsatzgeschäft gem. § 312c BGB ausschließlich unter Zuhilfenahme von Fernkommunikationsmitteln zustande kommt.
QR-Code 36

GEWÄHRLEISTUNGSRECHT
Ganz allgemein versteht man unter Gewährleistung die Rechte des Käufers oder der Käuferin beziehungsweise Verbaucher:in, die er oder sie bei einer mangelhaften Ware hat.
QR-Code 37

EHI
Zertifizierungspartner des Bundesverband E-Commerce und Versandhandel Deutschland e.V.
QR-Code 38

IPS
Online-Gütesiegel für Webseiten jeder Art und alle Branchen.
QR-Code 39

PHISHING
Phishing bedeutet, dass Daten von Internetnutzer:innen bspw. über gefälschte Internetadressen, E-Mails oder SMS abgefangen werden. Die Absicht ist, persönliche Daten zu missbrauchen und Inhaber von Bankkonten zu schädigen.
QR-Code 40

datenschutz und netzpolitik: was wissen konzerne wie amazon oder netflix über mich?

Copyright: Gordon Welters

Katharina Nocun, Publizistin, Wirtschafts-und Politikwissenschaftlerin.

Das tägliche Online-Verhalten ist geprägt von Informationssuche, Produktkäufen, Interaktionen auf sozialen Netzwerken und den vielen weiteren Nutzungsmöglichkeiten des Internets. Jegliches Verhalten im Netz hinterlässt einen sogenannten "digitalen Abdruck" der Nutzer:innen, den Plattformen für verschiedene Zwecke verwenden können. Welche Informationen Konzerne wie Amazon, Netflix oder Facebook über Personen anhand ihrer Datenspur sammeln können, wie sie dieses Wissen nutzen und wie sich dies auf Endverbraucher:innen auswirkt, wird im Folgenden dargestellt. Katharina Nocun hat einen Selbstversuch gemacht und beleuchtet in ihrem Buch, "Die Daten, die ich rief: Wie wir unsere Freiheit an Großkonzerne verkaufen", wie tiefgreifend die Datenspur ist, die sich Konzerne zunutze machen. Die Auszüge präsentierte sie in der Keynote des Online-Seminars.

Datenspur und gesetzliche Regelungen

Im Grunde können alle Nutzer:innen auf Basis der dafür geltenden gesetzlichen Grundlage die eigene Datenspur herausfinden. Diese Gesetzesgrundlage ist in der EU Datenschutzgrundverordnung Artikel 15 zu finden. Danach kann man jederzeit ein Unternehmen kontaktieren und eine kostenfreie Kopie der gespeicherten Daten anfordern.

QR-Code 1

Beispiel einer Datenspur anhand der Deutschlandcard

Die Deutschlandcard ist eine Punkte-Sammelcard, welche man bei Einkäufen verwenden kann. Meldet man sich auf dem Online-Portal an, kann man dort die Anzahl der gesammelten Punkte sehen. Auf Anforderung bekommt man die Auflistung dessen, was man eingekauft hat, eine grobe Artikelbezeichnung mit Artikelnummer, ebenso wie eine Zuordnung der entsprechenden Punkte. Jeder Artikel, den man kauft, ist dem entsprechenden Namen, Geburtsdatum und Adresse zugeordnet.

Bei regelmäßigen Käufen von einem bestimmten Produkt können Nutzer:innen dank dieser Daten einen Rabattgutschein für Produkte oder Werbung für ähnliche Artikel erhalten.

Anhand von Datensammlungen können gleichermaßen intime Dinge über eine Person ersichtlich werden, wie das folgende Beispiel eindrucksvoll aufzeigt.

Fallbeispiel einer Drogeriekette in den USA

Es gibt in den USA eine Drogeriekette, welche verschiedene Produkte verkauft und über ein Rabattsystem verfügt. Diese Drogeriekette versendet personalisierte Werbung an Kunden und Kundinnen, die auf Basis ihrer Datenanalyse mit hoher Wahrscheinlichkeit die jeweiligen Personen interessiert. Zum Beispiel interessieren sich einige Menschen eher für Nahrungsmittel, während andere sich eher für Nahrungsergänzungsmittel interessieren.
Eines Tages rief ein ziemlich verärgerter Herr bei der Drogeriekette an, der die Geschäftsleitung sprechen wollte. Er klagte über Werbung für Schwangerschaftsprodukte, die seine Tochter bekäme. Sie sei noch minderjährig und habe mit Geschlechtsverkehr und Schwangerschaft nichts zu tun. Er warf dem Geschäftsführer vor, seine Tochter zu vorehelichem Geschlechtsverkehr verlocken zu wollen.
Eine Woche später stellte sich jedoch heraus, dass die Tochter in der Tat schwanger war, woraufhin sich der Herr bei der Geschäftsleitung entschuldigte. An diesem Beispiel sieht man, dass Unternehmen manchmal noch vor Familienmitgliedern relativ intime Angelegenheiten von Kunden und Kundinnen mitbekommen können.

Wie konnte das Unternehmen wissen, dass das erwähnte Mädchen schwanger war?

Die Drogeriekette hat einen riesigen Datensatz tausender Kunden und Kundinnen. Oft werden Datensätze auch von externen Quellen angereichert, d.h. weitere Daten hinzugekauft.
Anschließend werden diese Daten analysiert und es wird ersichtlich, dass einige Kundinnen ab einem bestimmten Zeitpunkt anfangen, Windeln, Babynahrung usw. zu kaufen. Diese Kundinnen haben also mit einer hohen Wahrscheinlichkeit ein Baby. Anschließend wird geprüft, ob bestimmte Kaufmuster in den neun Monaten vor dem ersten Windel- und Babybreikauf zu erkennen sind. Und tatsächlich gibt es ca. ein Dutzend Veränderungen im Kaufverhalten von werdenden Müttern. So kann man am Kaufverhalten einer Frau erkennen, dass sie wahrscheinlich schwanger ist und davon weiß.
Durch die Analyse von **Big Data** kann man sehr intime Dinge von Personen herausfinden. Hierbei schaut man bei den Daten von einer Vielzahl von Menschen nach Auffälligkeiten. Diese kann man übertragen und daraus Schlüsse ziehen. Das Modell kann falsch liegen, aber auch erstaunlich oft richtige Einschätzungen treffen.
Mit diesem Wissen können sich Kund:innen entscheiden, ob sie z.B. die Deutschlandcard verwenden möchten oder nicht. Bei Käufen, die sehr persönliche Produkte umfassen, würden die meisten wahrscheinlich darauf verzichten.

QR-Code 2

Datenspur bei Online-Käufen

Online-Käufe lassen sich mit einer Supermarkt-Situation vergleichen, bei der der Kunde oder die Kundin beim Einkaufen permanent von Mitarbeitenden beobachtet werden würde. Ein Kauf könnte demnach folgendermaßen protokolliert werden:
Eine Kundin oder ein Kunde nimmt eine Chips-Packung aus dem Regal, guckt sich die Kalorientabelle an, stellt die Packung wieder zurück und nach zehn Minuten kehrt er oder sie wieder an den ursprünglichen Ort zurück und tut die Packung doch in den Wagen oder bleibt sehr lange vor einem Regal stehen, kauft aber nichts davon.
Online können Beinahe-Käufe, Recherchen und weitere Faktoren eingesehen werden, die über die Datenspur in einem Supermarkt hinausgehen. Auf Plattformen wie Amazon kann man die eigene Datenspur anfordern. Oft erhält man eine verschlüsselte CD-Rom mit einem Passwort, auf welcher unterschiedliche Datensätze zu finden sind.

Was lässt sich aus einem Datensatz herauslesen?

In einem Datensatz kann man Werbeanzeigen einsehen, welche sich ein Kunde oder eine Kundin angeschaut hat. Man kann Links nachverfolgen, die eine Person aus Werbemails angeklickt hat. Es wird auch der **Click-Stream** einer Person dokumentiert. Damit wird jeder Click ersichtlich, den eine Person auf einer Seite getätigt hat. Jede angeschaute Rezension, jedes angesehene Bild, jeder angeschaute Kommentar, jede Suchanfrage ist protokolliert.
Aus diesen Daten kann man schließen, an welchen Tagen die Käufer:innen nur schauen, weil es ihnen z.B. langweilig ist und an welchen Tagen tatsächlich Käufe getätigt werden. So kann ein Unternehmen passende Rabattgutscheine an die Kunden verschicken.
Anhand der **IP-Adresse** ist ersichtlich, in welchem Bundesland und welcher Stadt sich eine Person befindet. So kann z.B. nachvollzogen werden, wohin eine Person reist oder wo sie arbeitet. Auch kann ersichtlich werden, wo die Familie oder naheste-hende Menschen einer Person leben, wenn man z.B. öfter Pakete an eine bestimmte Adresse verschickt oder sich an Weihnachten dort aufhält. Die Namen der Netzanbieter werden ebenfalls erfasst. So können Daten bis ins Private eindringen. Durch **VPN** Anbieter kann man die IP-Adresse verschleiern, was jedoch nur die wenigsten tun.
Das Wissen von Plattformen wie Amazon geht darüber hinaus, was man auf der Plattform selbst macht. Ist man z.B. auf einer Artikelseite und klickt auf eine dort angezeigte Werbung und kommt so auf Amazon, so wird der gesamte Weg im Datensatz ersichtlich. Es ist also auch zu erkennen, welche Interessen eine Person außerhalb der Plattform hat.
Innerhalb der Plattform lässt sich ebenfalls auf mögliche Interessen schließen, wenn man z.B. die Bücher sieht, die eine Person liest oder die Spiele, die eine Person spielt. So lässt sich sagen, welche Vorlieben, Geschmäcker oder gar politische Ansichten eine Person hat. Problematisch ist dabei, dass ein Datensatz keine Erklärungen erhält und missinterpretiert werden könnte.

QR-Code 3
QR-Code 4
QR-Code 5

Datenspur bei Streamingdiensten

Netflix ist ein prominentes Beispiel für Streamingdienste. Fragt man hier nach einer Datenspur, so bekommt man einen Click-Stream, der darüber Auskunft gibt, wann man sich überlegt hat, welche Filme anzuschauen. Man sieht, welche Suchbegriffe eingegeben wurden und welche Trailer angeschaut wurden.
Auf weitere Nachfrage kann man auch die Übersicht von Angaben erhalten, welche zeigen, wann man wo vor- oder zurückgespult hat und wo man auf Pause gedrückt hat. Man kann also sehen, welche Szenen übersprungen wurden und welche doppelt und dreifach wiederholt angeschaut werden. Daraus kann man Schlüsse über private Informationen einer Person ziehen. Beispielsweise kann man ableiten, in welcher emotionalen Verfassung sich eine Person zum Zeitpunkt befand, an dem sie sich etwas angeschaut hat und welche Vorlieben und Neigungen sie wahrscheinlich hat.
In den vergangenen Jahren hat Netflix mit einem innovativen Videokonzept experimentiert. Darin gab es Filme, in denen Zuschauer:innen selbst Entscheidungen treffen konnten. Man spielt einen Charakter im Film und je nachdem, wie man sich entscheidet, folgt eine bestimmte Videosequenz. Man bestimmt somit die Handlung des Filmes mit.
Die Entscheidungen, die man als Zuschauer:in trifft, sind anfangs harmlos, wie z.B. „Welche Haferflocken möchtest du vom Frühstücksbuffet?“ Die Fragen verstricken sich jedoch schnell und können über Leben und Tod bestimmen.

QR-Code 6

Einfluss der EU-Datenschutzverordnung auf Datenanfragen

Dank der EU-Datenschutzverordnung ist es einfacher, Datenanfragen zu stellen. Mittlerweile kann man Datenanfragen via E-Mail stellen. Teilweise bekommt man Zugriff auf Daten in verschlüsselter Form über einen Downloadlink.
Die Reaktionszeit auf Anfragen ist gesunken, denn es gibt Regelungen zum bewussten Verstoßen oder Ignorieren des Datenschutzes. Es gibt Aufsichtsbehörden, an welche sich Verbraucher:innen im Falle eines Gesetzesverstoßes wenden können.
Die Debatte um ein neues europäisches Datenschutzgesetz hat das Bewusstsein für Betroffenenrechte geschaffen und das Interesse der Menschen an ihren eigenen Daten erhöht.

Welches Interesse steht hinter Datensammlungen?

Größere Konzerne haben Geschäftsbereiche, bei denen Big Data einen sehr großen Unterschied machen kann, beispielsweise, wenn es um künstliche Intelligenz geht. Je mehr Daten man für solch ein System verwendet, desto größer wird der Vorsprung gegenüber der Konkurrenz.
Im Bereich Marketing nutzt man die Daten für psychologische Profilings, um passende Werbemaßnahmen zu ergreifen, die Kund:innen sowohl positiv wie auch negativ beeinflussen können.
In bestimmten Fällen greifen staatliche Behörden auf Datensammlungen zurück, wobei die Grenzen zwischen staatlichen und privaten Datensammlungen immer weiter verschwimmen. Der Skandal um den Whistleblower Edward Snowden ist ein gutes Beispiel dafür, wie staatliche Behörden sowohl bei Google wie auch bei Facebook von Zugriff auf Daten Gebrauch machen.
Im politischen Bereich gab es bereits große Diskussionen in Bezug auf Werbebotschaften vor Wahlen. Das Unternehmen Cambridge Analytica nutzte Microtargeting, um Menschen gezielte Werbebotschaften anhand ihrer Präferenzen anzuzeigen. Inwiefern dies Auswirkungen hatte, ist fraglich. Insbesondere bei knappen Entscheidungen können wenige Prozente viel ausmachen und eine sehr wichtige Entscheidung, wie zum Beispiel die Wahl der Regierung oder den Beitritt eines Landes in die EU, beeinflussen.

QR-Code 7
QR-Code 8
QR-Code 9

Mastodon – Alternatives soziales Netzwerk

Bei Mastodon handelt es sich um ein soziales Netzwerk, hinter dem kein Unternehmen steht. Es ist eine freie Software, die den Datenschutzgesetzen Deutschlands unterliegt.

So funktioniert Mastodon:

> Jede:r kann auf einem eigenen Server das dezentrale Netzwerk - Mastodon (Software) aufsetzen. Diese Netzwerke kommunizieren miteinander.
> Der Administrator vom Server kann von jedem oder jeder ausgesucht und gewechselt werden.
> Unterschiedliche Plattformen haben unterschiedliche Regeln.
> Es wird viel Rücksicht auf verschiedene Themen gelegt, im Gegenteil zu größeren Plattformen, bei welchen es oftmals weniger Regulierung gibt.

Datensätze anfordern

Um einen Datensatz von einem Unternehmen anzufragen, reicht es aus, eine E-Mail zu schreiben. Man sollte seine Kundennummer nennen und sich auf Artikel 15 der Datenschutzverordnung (das Auskunftsrecht) beziehen. Es ist vorteilhaft, eine Frist von einem Monat zu setzen, um eine zeitnahe Antwort zu erhalten.

Data Literacy

Die Datensätze sind in der Regel ohne Vorkenntnisse im Bereich Datenschutz relativ schwer zu deuten. Ohne Expert:innen oder Software zur Auswertung geht man leicht verloren. Deshalb wäre es sinnvoll, Unternehmen in die Pflicht zu nehmen, die Datensätze so aufzubereiten, dass man sie ohne Vorwissen verstehen kann.

QR-Code 10

Gefahren von Profilings

> Politische Werbebotschaften anhand von psychologischen Profilings vor Wahlen können das Vertrauen der Menschen in die Demokratie gefährden, da diese in ihrer Entscheidung beeinflusst werden.
> Datenpannen können im schlimmsten Fall zur Veröffentlichung der Daten führen.

Kann man sich dem Profiling entziehen?

> Sich politisch für eine stärkere Regulierung von Profiling einsetzen
> VPN-Anbieter nutzen
> Auf Rabattsysteme verzichten
> Alternative Suchmaschinen nutzen
> Geschäftsbedingungen von Plattformen wie Facebook kennen

Dies alles sind Wege, die das Problem der Datenverarbeitung nur teilweise beseitigen, weshalb es vorteilhaft wäre, eine ganzheitliche politische Lösung zu finden.

cybermobbing - strategien dagegen und prävention

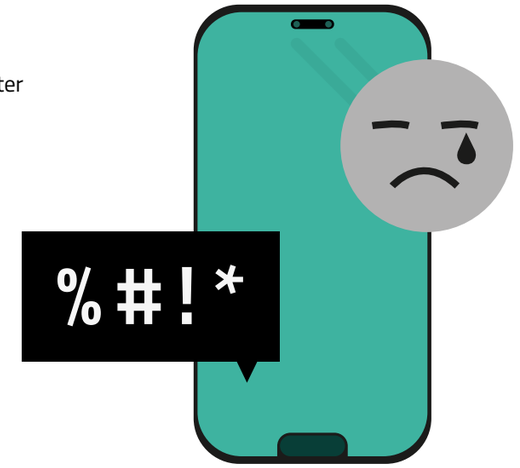
Copyright: Oliver Nauditt

Lukas Pohland,
Cybermobbing-Hilfe e.V

Unter Cybermobbing versteht man Hass, Beleidigungen und Bedrohungen in digitalen Räumen, welches durch ein anderes Ausmaß und andere Konsequenzen charakterisiert ist als Mobbing im Offline-Kontext. Wie man mit Cybermobbing umgehen kann, welche Lösungsansätze es gibt, was Betroffene und ihr Umfeld dagegen tun können und wie Täter:innen bestraft werden können, sind die folgenden Kernfragen. Lukas Pohland war selbst von Cybermobbing betroffen und hat beschlossen, mit der Gründung seines Vereins aktiv zu werden.

CYBERMOBBING HILFE

Allein in Deutschland sind schätzungsweise zwei Millionen Schüler und Schülerinnen von Cybermobbing betroffen. Im Gegensatz zum Mobbing in der realen Welt endet das Cybermobbing auch zuhause nicht, da die Handys, Tablets und Computer weiter genutzt werden und viele wichtige soziale Funktionen erfüllen.



Umgang mit Cybermobbing

Wie erkennt man, dass man sich in einer Mobbingsituation befindet?

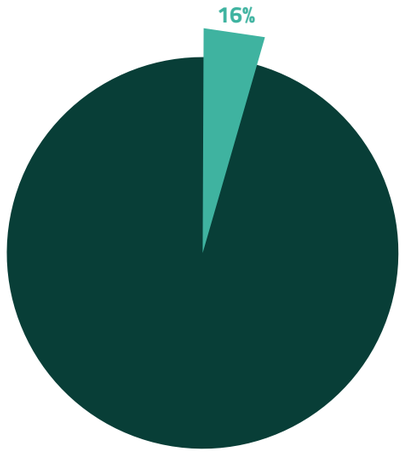
> Wiederholungscharakter
> Beleidigungen, Drohungen etc. über einen längeren Zeitraum
> Häufig greift eine Gruppe Einzelpersonen an (Stärkere gegen Schwächere)

Wie verhält sich ein Kind, das gemobbt wird?

> Änderungen im Verhalten
(z.B.: Essverhalten, Nutzung vom Smartphone, Schulängste)
> Psychische Folgen
> Schwänzen

Herausforderungen

1. Von außen ist es nur schwer zu erkennen, wenn jemand zum Opfer von Cybermobbing wird. Die Opfer verspüren oft ein Schamgefühl und berichten nicht von ihren Problemen. Manchmal denken Betroffene auch, dass die Täter:innen im Recht sind, was noch mehr belastet und ebenfalls zum Schweigen führt.
2. Gelegentlich werden Opfer aufgrund des mangelnden Verständnisses älterer Generationen nicht gehört. Sie können nicht verstehen, wieso das Mobbing als dermaßen belastend wahrgenommen wird. Es fehlt an Sensibilisierung.
3. **16% der Betroffenen, die Hilfe suchen, erhalten keine Unterstützung oder werden nicht ernstgenommen.** Hier besteht Aufholbedarf. Es ist außerdem wichtig zu vermitteln, dass sich Betroffene so früh wie möglich Hilfe suchen sollten, da das Cybermobbing im Anfangsstadium in vielen Fällen noch relativ unkompliziert gestoppt werden kann.
4. Digitale Räume werden von Lehrer:innen und Eltern oft nicht richtig verstanden, was das Problem umso gravierender macht. Oft möchten Kinder und Jugendliche vermeiden, dass Erwachsene mitbekommen, was sie in digitalen Räumen tun.



Im Juni 2017 wurde der Verein Cybermobbing Hilfe e.V. gegründet, an den sich von Cybermobbing betroffene Kinder und Jugendliche wenden können, um sich beraten zu lassen.

Welche Lösungsansätze gibt es für diese Herausforderungen?

> Kinder und Jugendlichen Freiraum schaffen, um sich in digitalen Räumen auszuprobieren
> Kontrolle von Erwachsenen vermeiden, stattdessen Bewusstheit schaffen
> Verständnis für die Sachlage bei Lehrer:innen und Eltern schaffen
> Kinder und Jugendliche dafür sensibilisieren, dass Mobbing in keinem Fall zu akzeptieren ist

Wie hilft der Verein bei Cybermobbingfällen?

> Offenes Ohr – Betroffene sprechen häufig zum ersten Mal aus, was passiert ist
> Aufbau von Selbstwertgefühl
> Praktische Ratschläge
> Vermitteln von Anlaufstellen für Betroffene vor Ort
> Hilfe bei der Kommunikation mit Lehrkräften und Eltern

Was können Plattformen tun?

> Konkrete Anlaufstellen für Betroffene schaffen
> Täter:innen konsequenter zur Rechenschaft ziehen (durch Justiz und durch Plattformen selbst)
> Ein deutlich ersichtliches Hilfsangebot auf den Seiten platzieren
> Das Problem kommunizieren
> Berater:innen für Betroffene zur Verfügung stellen

Wird Cybermobbing durch das Geschäftsmodelle der Plattformen begünstigt?

Bei Social Media Plattformen handelt es sich nicht um öffentliche Infrastrukturen, sondern um Unternehmen mit wirtschaftlichem Interesse. Diese möchten User und Userinnen möglichst lange auf der Plattform halten, was sowohl durch interessanten Content als auch durch Cybermobbing erreicht werden kann. Genau das ist ein großes Problemfeld, das den Plattformbetreibern bekannt ist, bislang jedoch relativ wenig zu einer Lösung beigetragen hat.

Begünstigen soziale Netzwerke das Cybermobbing?

Die Medien, auf denen Cybermobbing am häufigsten stattfindet, sind deckungsgleich mit den Medien, die von Kindern und Jugendlichen genutzt werden.
Whatsapp, Messenger und öffentliche soziale Medien wie Instagram bis hin zu Snapchat und Tiktok werden für Cybermobbing bevorzugt genutzt. Aber auch andere Medien wie z.B. Tellonym sind zu erwähnen. Tellonym ermöglicht es, anonym Nachrichten zu verschicken, was für Cybermobbing und andere digitale Straftaten förderlich ist.

Was kann das Umfeld von Betroffenen tun?

> Offenes Ohr anbieten
> Unterstützung anbieten / Betroffene auf dem Lösungsweg begleiten
> In der Schule mit dem Kind vorsprechen / Lehrkräfte ansprechen
> Sensibilisierung für das Thema
> Zurückhaltung in manchen Fällen (nicht die Täter:innen direkt konfrontieren)
> Ggf. Strafanzeige bei Polizei erstellen

Wie können Täter:innen bestraft werden?

> Schulen sind in der Pflicht, Ordnungsmaßnamen zu erwirken (es soll bei Täter:innen eingegriffen werden, statt nach der Lösung bei Opfern zu suchen)
> Nutzung der Strafbestände von Betroffenen und von Verfolgungsbehörden
> Erweiterung von Hilfemaßnahmen seitens der Behörden

Was können Betroffene tun?

> Frühzeitig Problem melden
> Anlaufstellen aufsuchen oder ansprechen
> Unterstützung suchen (Freunde, Eltern, Lehrkräfte)
> Beweise erstellen (Screenshots von Angriffen, Mobbingtagebuch erstellen mit Zeitangaben)
> Stärke zeigen, keine Angriffsfläche bieten
> Zivilcourage
> Strafanzeige einreichen

Wie können Jugendliche, Lehrkräfte und Eltern von der Anlaufstelle erfahren?

Auf der Webseite Cybermobbing-hilfe.de gibt es Ratschläge und Optionen, Ansprechpartner:innen direkt zu kontaktieren und eine Beratung anzufordern. **QR-Code 11**

internet ohne grenzen? wie der digital services act (dsa) das internet regulieren möchte.

Dr. Daniel Holznagel,
Richter am Landgericht Berlin.

Hat zu diesem Thema beim ZWST referiert. Nachfolgend wird wiedergegeben, was wir diskutiert haben.

Eine lange Zeit vorherrschende mangelhafte Regulierung von Onlineräumen, Hate Speech, Cybermobbing und weitere Problematiken im Internet sollen durch den Digital Services Act auf gesetzlicher Ebene adressiert und EU-übergreifend geregelt werden. Dr. Daniel Holznagel war bereits in der Vergangenheit an der Entwicklung von Gesetzen beteiligt, die die Regulierung von Online-Räumen sicherstellen sollen. Was genau der Digital Services Act bewirken soll, wie er zustande gekommen ist, wen er betrifft und wo er wirksam ist, wird im Weiteren ausgeführt.

Senatsverwaltung für Justiz und Verbraucherschutz BERLIN

Vorgeschichte und Entstehung des Digital Services Act

> Mitte der 90er-Jahre wird das Internet zu einem relevanten Feld und somit zu einem Regulierungssobjekt für die Politik.

> Wichtiges Anliegen damals: Die damals noch kleinen Start-ups vor Haftungsrisiken zu schützen.

> Für Plattformanbieter wurden zwei Kern-Privilegien abgesichert:

1. Inhalte wie Musik oder Filme müssen nicht geprüft werden, bevor sie veröffentlicht werden. Erst, wenn die Plattformen auf konkret Illegalität hingewiesen werden, müssen sie tätig werden.
2. Dienste dürfen grenzüberschreitend angeboten werden, es gilt für die Plattformen im Zuge des Herkunftslandsprinzips weitgehend nur das Recht des Landes, in dem sie ihren Geschäftssitz haben (one-stop-shop-Ansatz).

> Die Folge: Anbieter wie Facebook, Twitter und Co. verlegen ihren Sitz nach Irland, was verschiedene Gründe haben kann. Allerdings ist auffällig, dass Irland bei der Aufsicht über die Anbieter sehr zurückhaltend ist (Beobachtende werfen den Anbietern “**cherry-picking**” vor).

> Um die Jahrtausendwende steigt **Filesharing** rasant an, wobei auch urheberrechtsverletzende Dateien geteilt werden, was die Musik- und Filmbranche zunehmend bedroht.

> Um das **Urheberrecht** und damit verbundene Industrien zu schützen, werden schließlich Mitte der 2000er Jahre wichtige Neuregelungen für eine stärkere Verantwortung der Plattformen geschaffen. Zielrichtung ist aber v. a. der Schutz des Geistigen Eigentums.

> Hass und Desinformation spielt als rechtspolitisches Problem eher eine untergeordnete Rolle. Dies ändert sich Mitte der 2010er Jahre (Hate Speech crisis). Als ein Hintergrund wird vermutet, dass die Empfehlungsalgorithmen zu dieser Zeit stark an Bedeutung gewonnen und reißerische oder provozierende Inhalte so gefördert werden.

> Der Digital Services Act zielt nicht zentral auf den Schutz des geistigen Eigentums, sondern v. a. auf den Schutz der Bürger:innen vor **Hate Speech**, sowie den Schutz demokratischer Prozesse vor Desinformation und einiges mehr. Es geht dem EU-Gesetzgeber aber auch darum, nationale Alleingänge wie mit dem NetzDG zu unterbinden.

Entwicklung des Digital Services Act

Der erste Vorschlag für das europäische Gesetzgebungsvorhaben des Digital Services Act wurde Ende 2020 vorgestellt und zügig auf europäischer Ebene diskutiert. Nach Zustimmungen der Verantwortlichen wurde im April 2022 der entscheidende Verhandlungsdurchbruch erzielt. Am 16. November 2022 ist das Gesetz in Kraft getreten. Es gilt voll ab dem 17. Februar 2024.

Zweck des Digital Services Act

Netzpolitik ist ein sich sehr dynamisch entwickelndes Feld der Politik, auf welches auch Bürger:innen Einfluss nehmen können und sollten.
Der DSA beinhaltet detaillierte Vorschriften mit verschiedenen Zielrichtungen, wobei das übergeordnete Ziel des Digital Services Act darin besteht, ein transparentes und sicheres Online-Umfeld zu schaffen und die Rechte der Nutzer:innen zu stärken.
So soll man zum Beispiel als Facebook-Nutzer:in bei einer als ungerecht empfundenen Sperrung oder Löschung des Accounts gestärkt werden. Es sollen in diesem Fall die Rechte der einzelnen Nutzer:innen, eine Überprüfung der Maßnahme zu erreichen, erweitert werden.
Sehr große Anbieter (Facebook, YouTube usw.) werden jährlich Risikoanalysen durchführen müssen (vereinfacht: welche Risiken für Bürger:innen und Gesellschaft erzeugt meine Plattform?) und auf erkannte Defizite reagieren, was behördlich überwacht wird.

Auswirkung des Digital Services Act

Nach dem Inkrafttreten des Gesetzes wird es für sehr große Anbieter zunächst eine Übergangsvorschrift von vier Monaten geben. Die Anbieter werden registriert und müssen ihr Verhalten entsprechend der neuen Gesetzgebung anpassen. Insgesamt und auch für kleinere Anbieter gilt der DSA ab dem 17.2.2024. Die Regelungen sind vor allem an Online-Plattformen gerichtet, bei denen ein Austausch zwischen Nutzer:innen, unter anderem in Form von Beiträgen, stattfinden kann.

Aktuelle Notwendigkeit des Digital Services Act

Da sich das Nutzungsverhalten in der Vergangenheit stark von dem heutigen unterschied, wurde dieser Problemstellung lange Zeit keine Aufmerksamkeit geschenkt, was wiederum auch für einen relativ ungestörten europäischen Rechtsrahmen sorgte. Online-Plattformen konnten gedeihen. Kleine Start-Ups wurden zu den wertvollsten Unternehmen der Welt.
2015 war die bestehende Rechtsregulierung offenkundig nicht mehr ausreichend. Zu diesem Zeitpunkt wurde ersichtlich, dass nicht nur Musikpiraterie betrieben wurde, sondern auch Hassdynamiken entstanden, gegen welche nicht genug von den Plattformen unternommen wurde.
Online-Rechts- und Persönlichkeitsverletzungen stiegen rasant an. Sie wurden zu einem bedeutenden Problem, das bis heute anhält.

Gründe für Entstehung von Hasswellen im Internet

Anhaltende und steigende Diskriminierungswellen in Europa haben sich zunehmend auch in digitalen Räumen Zugang und Präsenz verschafft. Eine wichtige Rolle spielen auch die Empfehlungs-Algorithmen der Plattformen. Das Engagement der Nutzer:innen mit den Inhalten der Plattformen hat stark an Bedeutung gewonnen. Bspw. eine emotionale Interaktion mit einem Post wird belohnt und von Plattformen durch häufigere Darstellung an noch mehr Nutzer:innen gefördert. So bekommen Beiträge, die viel Aufsehen und Empörung erregen, oft viel Aufmerksamkeit.
Zu den Posts, auf die Nutzer:innen am meisten reagieren, gehören solche mit kontroversen Inhalten. Da beispielsweise Beiträge, die Beleidigungen beinhalten, mehr Interaktionen generieren, werden sie durch den Algorithmus sichtbarer gemacht und tragen dadurch zur Entstehung von Hasswellen bei.

Maßnahmen gegen Hasswellen im Internet

Maßnahmen der Plattformen
Ab 2018/19 wurde bei Facebook erheblich in die Bereiche Sicherheit und Moderation investiert. Es wurden Mitarbeiter:innen mit entsprechendem Sprach- und Kulturverständnis eingestellt. Auch andere Plattformen verstärkten ihre Maßnahmen. Die Plattformen reagierten damit auf den stärkeren politischen Druck, u.a. dass die Gesetzgeber in Europa Überlegungen zu Gesetzen aufnahmen oder z.B. wie in Deutschland mit dem NetzDG in 2017 bereits verabschiedeten.

Maßnahmen der Betroffenen
Nutzer:innen können bei Beleidigungen u.ä. zivilrechtlich vorgehen. Nur wenige machen von dieser Möglichkeit jedoch Gebrauch, da die Kosten und Risiken bei solchen Klagen sehr hoch sind. Deshalb ist das Problem der Persönlichkeitsverletzung durch Hassrede usw. zivilrechtlich allein nicht lösbar, es braucht hier staatliche/behördliche Unterstützung. Bei Urheberrechtsklagen hingegen, bei denen es um geistiges Eigentum geht, ist juristische Vorgehen deutlich wirkungsvoller (es gibt oft bedeutenden Schadensersatz, zudem sind die Rechteinhaber gut organisiert und haben oft hinreichende Ressourcen für Rechtsstreite).

Maßnahmen der Politik
Ab 2016 wurde das Hassproblem im Internet von der Politik wahrgenommen, woraufhin es einen Beschluss in Deutschland gab, das NetzDG einzuführen.

Durch das NetzDG wurden vier Bereiche geändert, die behördlich überwacht werden:

1. Nutzerfreundlichere Meldewege (Per Klick zur Hassmeldung bei YouTube und Co.)
2. Vorgaben für die Plattformen, auf Beschwerden zu reagieren
3. Transparenz bezüglich der Moderationsentscheidungen
4. Erleichterte Kontaktaufnahme durch inländische Kontaktpersonen

Weitere EU-Länder wie Frankreich und Österreich sind dem Beispiel gefolgt und haben ähnliche Gesetze verabschiedet. Da die EU aber den Binnenmarkt erhalten und einen einheitlichen Rechtsrahmen schaffen möchte, in dem Dienste frei grenzüberschreitend erbracht werden können, kam 2020 der Vorschlag, den Digital Services Act einzuführen.

Aktuelle Informationen zum DSA: QR-Code 16

Schwachstellen und Stärken der neuen Gesetzgebung

Die Vorschrift der regelmäßigen Selbsteinschätzung von Risiken bei großen Plattformen könnte problematisch in der Umsetzung werden. Es könnte zu einer Abwehrhaltung seitens der Plattformbetreiber kommen, gegen welche es schwer sein wird, die Vorschrift durchzusetzen.

In den kommenden Jahren wird es deshalb wahrscheinlich schwer sein, diese Regelung wirksam durchzusetzen. Der große Fortschritt der neuen Gesetzgebung besteht darin, die Zuständigkeit von Irland für die großen Plattformen zu entziehen und sie in europäische Kommissionen zu übergeben.

Wichtige Änderungen der Sachlage durch den Digital Services Act

1. Notwendigkeit einer Begründung für Moderationsentscheidungen
2. Die Möglichkeit, Beschwerden einzulegen gegen eine Entscheidung
3. Die Möglichkeit einer außergerichtlichen Streitbeilegung, die sehr günstig für Verbraucher:innen ist
4. Transparenzvorgaben
5. Werbung auf Online-Plattformen muss sehr transparent gestaltet werden (Auftraggeber, Parameter zur Auswahl der Nutzergruppe usw.) Beschränkung von targeted-ads
6. Erschaffung eines Archivs für Online-Werbung
7. Eigener Datenzugang für Wissenschaftler:innen
8. Kontaktpersonen im Herkunftsland sollen durch eine Kontaktperson in der EU ersetzt werden
9. Konkrete Zeitvorgaben zur Löschung von gesetzwidrigen Inhalten werden behoben
10. Regelmäßige Selbsteinschätzung von Risiken für große Anbieter ab 45 Millionen Nutzer:innen

Wesentlicher Antrieb für die Entstehung des Digital Services Act:

1. Verhinderung der Fragmentierung in der EU
2. Sicherer Online-Rechtsrahmen

Reaktion der Plattformbetreiber auf den Digital Services Act
Die Plattformen wollen juristische Auseinandersetzungen meiden und sind an klaren Regelungen interessiert, die konstant befolgt werden können. Ebenfalls ist es für die Plattformbetreiber von Vorteil, eine europaweite Gesetzgebung zu befolgen und sich nicht an die Gesetze jedes einzelnen Landes anpassen zu müssen. Zum einen können Konzerne so Kosten sparen und zum anderen die Vorzüge der europäischen Gesetzgebung genießen, welche sich letztlich für die Anbieter als nicht zu streng erweisen dürfte. Deshalb ist davon auszugehen, dass die neue Gesetzgebung von den Plattformbetreibern angenommen wird.

Einfluss der Nutzer:innen auf den Digital Services Act
Es wird Konsultationsprozesse geben, in welche Bürger:innen sich einschalten und so mitwirken können. Zudem ist zu beachten, dass wir alle Teil eines Netzwerks darstellen und somit auch den Mehrwert einer Plattform bilden. Nutzer:innen haben hier also Rechte wie in einer Demokratie, dies könnte in Zukunft stärker in den Mittelpunkt rücken (evtl. auch in Gerichtsverfahren).

Einschätzung der Wirksamkeit des Digital Services Act
Plattformen sind laut dem Digital Services Act dazu verpflichtet, die Entscheidungskriterien der Algorithmen transparent zu gestalten. Dennoch bietet die Regelung an dieser Stelle noch große Freiräume. Wissenschaftler:innen Zugang zu gewähren, ist wichtig und kann sich als wirkungsvoll erweisen, da die Plattformen bisher als unzugängliche Black Box betrachtet wurden.
Bei der zentralen Regelung (der Risikobewertung der Plattformen) hängt viel von Behörden ab, konkrete Risiken zu identifizieren und anzusprechen. Der Fortschritt wird hier auf die Vorgehensweise der Behörden zurückzuführen sein.

Weiterführende Informationen zum aktuellen Status des Digital Services Act:
Weitere Informationen QR-Code 17

sicher durch digitale lebenswelten


Copyright: Andi Weiland

Dr. Michael Littger, Geschäftsführer, Deutschland sicher im Netz e.V

Zunehmend viele Lebensbereiche werden digitalisiert. Dazu gehören das Einkaufsverhalten, die Arbeitsmodalitäten, Bildung oder Ehrenamt. Besonders für vulnerable Zielgruppen sind mit diesem Wandel Herausforderungen verknüpft. In der folgenden Übersicht wird aufgezeigt, wie man sicher durch die verschiedenen digitalen Räume navigiert und welche Initiativen beim bewussten und informierten Medienkonsum unterstützen können.

DsiN Deutschland sicher im Netz

Bereiche des Lebens im digitalen Raum – Was gilt es zu beachten?

Verkehr und Mobilität
> Mobile Anwendungen ermöglichen Betreibern die Erhebung von Daten über das Fahrverhalten, den Standort oder Reisepräferenzen von Verbraucher:innen. Wichtig ist hierbei das Bewusstsein um Optionen und Einstellungen, die es ermöglichen, die Datenerhebung zu steuern und einzuschränken.

Digitales Shopping
> Tagtäglich kaufen Menschen online ein, das eigene Nutzerkonto, Bankkonto und der E-Mail-Account sollten dabei durch Passwort-geschützte Zugänge abgesichert werden. Passwortmanager und Sicherheitseinstellungen, wie die Zwei-Faktor-Authentifizierung sind hierbei wichtige Instrumente..

Arbeitswelt und Homeoffice
> Die Option von zuhause aus zu arbeiten, wurde insbesondere während der Pandemiezeit genutzt. Der Schutz von Organisationsdaten ist dabei besonders kritisch.

Bildung und Schule
> Unterricht kann mit digitalen Mitteln zunehmend anschaulicher gestaltet werden. Außerdem ist es wichtig, die Informations- und Recherchekompetenz bei Schüler:innen zu fördern und sie im Umgang mit Desinformation im Internet zu wappnen.
> DigiBitS ist ein Programm für allgemeinbildende Schulen, dass es den Lehrkräften ermöglicht digitale Kompetenzen zu vermitteln.

Zivilgesellschaft und Ehrenamt
> Themen wie digitale Mitgliederverwaltung oder Sicherheit beim Fundraising sind zentrale Herausforderungen für soziale Akteure.

Initiativen, die im sicheren Medienkonsum unterstützen:

Klicksafe
hat zum Ziel, die Online-Kompetenz der Menschen zu fördern und sie beim kompetenten und kritischen Umgang mit dem Internet zu unterstützen.
QR-Code 19

Digitaler Engel
Mit dem Projekt Digitaler Engel unterstützt **„Deutschland sicher im Netz“** ältere Menschen bei der Nutzung digitaler Angebote
QR-Code 20

Digital-Kompass
Um die vielfältigen Chancen der Digitalisierung für Menschen mit Beeinträchtigungen verständlich und erlebbar zu machen, bietet der Digital-Kompass vielfältige Angebote, wie digitale Lern-Tandems in den eigenen vier Wänden und Beratung durch qualifizierte Engagierte in Treffpunkten vor Ort.
QR-Code 21

PolisiN
„Politiker:innen sicher im Netz“ richtet sich an Politiker:innen und Mitarbeiter:innen in Parteien, Fraktionen, Büros sowie Verwaltungen auf Bundes-, Landes- und kommunaler Ebene.
QR-Code 22

Digitalführerschein
Der DsiN-Digitalführerschein (DiFü) zertifiziert das Wissen rund um die digitalen Themen des Alltags.
QR-Code 23

social media und jugendschutz

Copyright: Silke Rudolph

Maja Wegener,
Geschäftsführerin,
Bundesarbeitsgemeinschaft
Kinder- und Jugendschutz.

Klaus Hinze,
Vorstandsvorsitzender,
Bundesarbeitsgemeinschaft
Kinder- und Jugendschutz.

In diesem Beitrag geht es um die Mediennutzung von Kindern und Jugendlichen, die Plattformen, die sie vermehrt nutzen, die damit verbundenen Risiken sowie gesetzlichen Grundlagen zum Schutz junger Menschen im Netz.

BAJ Bundesarbeitsgemeinschaft Kinder- und Jugendschutz

Medien, Digitalisierung und ihre Auswirkung auf Kinder und Jugendliche

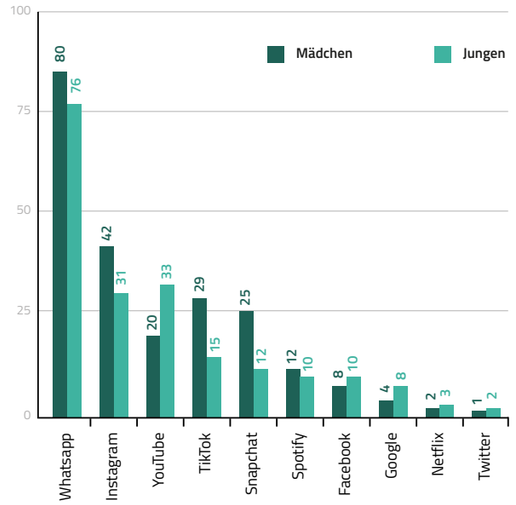
Wir alle verwenden mediale Räume wie z.B. Filme, soziale Netzwerke oder Videospiele. Mediale Räume brachten schon immer auch die Jugendkultur zum Ausdruck. Kinder wachsen mit Figuren aus Zeichentrickfilmen auf, mit denen sie sich identifizieren können. Heute sind mediale Räume zudem stark durch Smartphones und Social Media geprägt.

Einfluss der Gesetzgebung

Bereits im Jahr 1920 wurde das erste Gesetz zum Jugendschutz verabschiedet: das ***Lichtspielgesetz*** sollte Menschen vor einer schädlichen Wirkung von Filmen bewahren. Kurz darauf folgte das *Gesetz zur Bewahrung der Jugend vor Schmutz- und Schundschriften* (1926), welches potentiell schädliche Einflüsse von Literatur auf Kinder und Jugendliche regulieren sollte. Das weiterführende *Gesetz zum Schutz der Jugend bei Lustbarkeiten* zielte auf Jugendschutz im öffentlichen Raum ab.
Im aktuellen Jugendschutzgesetz regelt §14a die Kennzeichnung bei Film- und Spieleplattformen, wobei die FSK für die Filme und die USK für Spieleplattformen zuständig ist.
Heute gilt das Jugendschutzgesetz (auf Bundesebene), das den Jugendschutz in Öffentlichkeit und den Medien regelt. Zielgruppe des Jugendschutzgesetzes sind Gewerbetreibende und Veranstalter.
Das zweite aktuell gültige Gesetz ist der Jugendmedienschutz-Staatsvertrag (auf Länderebene). Dieses Gesetz wird derzeit reformiert. Es gilt für den Bereich von Telemedien im privaten Rundfunk, Fernsehen und im Internet.

QR-Code 24
QR-Code 25

Wichtigste Apps 2021
- bis zu drei Nennungen ohne Antwortvorgabe



Quelle: JIM 2021

Die Mediennutzung junger Menschen

Die jährliche JIM-Studie (Jugend, Information, Medien), die vom Medienpädagogischen Forschungsverbund Südwest erstellt wird, untersucht die Mediennutzung junger Menschen. Dabei wird die Altersgruppe der 12- bis 19-jährigen erfasst.
Die zweijährlich erscheinende KIM-Studie (Kindheit, Internet, Medien) befasst sich mit der Mediennutzung der 6- bis 12-Jährigen. Sie zeigt auf, in welchen digitalen Räumen sich Kinder bewegen. Es wird ein Überblick über soziodemografische Daten bereitgestellt.
Im Jahr 2021 ist die Whatsapp-Nutzung bei jungen Menschen im Vergleich zum Vorjahr gestiegen. Enorm zugenommen hat auch die Nutzung vom Instagram als Social Media Plattform. Bei Tiktok ist ein leichter Rückgang zu beobachten. Snapchat hingegen genießt wieder mehr Beliebtheit. Dies sind die zentralen Apps, die das Nutzungsverhalten der Jugendlichen aktuell bestimmen.

QR-Code 26
QR-Code 27

Blick des Jugendschutzes:
Medien im Wandel *(Hajok/Lauber 2013)*

Mobile Endgeräte mit Internetzugang
> Laptops, Smartphones, Tablets, Konsolen, etc.

Gesellschaftliche und kulturelle Teilhabe
> Foren, Bolgs, Youtube, Instagram, etc.

Digitalisierung neuer und alter Inhalte
> mitsamt Übertragung in andere Nutzungskontexte

Spektum der Möglichkeiten erweitert
vieles kann genutzt werden

nur wenig wird genutzt
Anbieterkonzentration und digitale Spaltung

Zunehmend dynamische Angebote
> User Generated Content, Kommentare, Likes, etc.

Selbstdarstellung, Kontaktpflege im Netz
> persönliche Profile, Online-Freundeskreise, etc.

Neue Formen der Wertschöpfung
> Virales Marketing, personalisierte Werbung, etc.

Das Informationsverhalten junger Menschen und Fake News

Laut verschiedener Untersuchungen vom Jahr 2021 stehen Suchmaschinen bei der Informationssuche ganz oben, wobei auch Instagram eine große Rolle spielt. Es folgen YouTube Videos, Google News und Tiktok.

An dieser Stelle wird deutlich, dass gewisse Risiken (Stichwort Fake News) mit der Nutzung dieser Plattformen einhergehen. So können zum Beispiel Verschwörungsglauben, die über Social Media verbreitet werden, Jugendliche (aber auch Erwachsene) in ihrer Meinung stark beeinflussen.

QR-Code 28

Räume zum Spielen

Minecraft, Fortnite und FIFA sind die beliebtesten Videospiele unter Jugendlichen. Bei älteren Spieler:innen kommen GTA und Call of Duty dazu, die eindeutig nur für Erwachsene zulässig sind.
Es ist ersichtlich, dass Spiele, die ab 18 freigegeben sind, selbst bei 16- bis 17-jährigen und oft auch schon bei 15-jährigen verbreitet sind.

Räume zum Lernen

Der Medienpädagogische Forschungsverbund hat eine Studie durchgeführt, die zeigt, dass in der Corona-Zeit, in welcher Jugendliche auch zum Lernen stark auf die digitalen Medien angewiesen waren, *YouTube* eine wichtige Rolle spielte. *Wikipedia* bekam als Lernmedium ebenfalls eine große Bedeutung.

Risiken bei der Online-Nutzung

1. Verbreitung von falschen Informationen über Personen (Tendenz steigend)
2. Fake News (Tendenz steigend)
3. Verschwörungsglauben, Verschwörungsmythen (Tendenz steigend)
4. Extremistische politische Inhalte (Tendenz steigend)

12- bis 15-jährige sind besonders stark betroffen.

Mediale Räume und der Jugendschutz

Phasen des Jugendschutzes bei der Onlinenutzung:

1. Internet (Webseiten, Chaträume)

Betrachtungsgegenstand:
unangemessene Inhalte, Foren zu selbstverletzendem Verhalten, Holocaustleugnung, Rassismus, gewaltverherrlichende Computerspiele

2. Social Media

Betrachtungsgegenstand:
illegale Downloads, Onlinespiele, Big Data / Datennutzung

3. Smartphone

Betrachtungsgegenstand:
permanente Erreichbarkeit, unkontrollierbare Kommunikation, Fake News, Hatespeech, Sexting, Cyber Grooming, Cybermobbing, Datafizierung

QR-Code 29
QR-Code 30
QR-Code 31

4. Digitales Smart Home/Digitales Kinderzimmer

Betrachtungsgegenstand:
Der Lebensalltag der Familien wird erfasst und durchdrungen durch Alexa, Siri u.Ä. - Tendenzen steigend

QR-Code 32

Am 1. Mai 2021 wurde das Jugendschutzgesetz mit einer Strategie für zeitgemäße und effektive Weiterentwicklung des Jugendmedienschutzes novelliert.

Unverändert blieb:
Jugendschutz in der Öffentlichkeit

JuSchG-Novellierung: Die Intentionen

> Modernisierung und Anpassung des Jugendschutzrechts an die Medienrealität
> Einführung eines konvergenten Medienbegriffs (Träger- und Telemedien)
> Benennung der Schutzziele und Erweiterung um Kommunikations- und Interaktionsrisiken
> Pflicht zur Anbietervorsorge für Betreiber von Plattformen (nutzergenerierte Inhalte ab 1 Mio. User)
> Pflicht zur Alterskennzeichnung für Film- und Spieleplattformen
> Gründung der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ)

Beim Jugendmedienschutz geht es nun nicht mehr allein um den Schutz, sondern darum, Kinder und Jugendliche, aber auch Eltern und Fachkräfte für das Leben im digitalen Raum zu befähigen und die Teilhabe im digitalen Raum zu ermöglichen. Hierbei werden beispielsweise Anbieter von Streaming- und Spieleplattformen stärker in Verantwortung gezogen.
In der Schule geht es um die Medienkompetenz. Sowohl Eltern als auch Kinder und Fachkräfte sollen im Umgang mit den Medien gestärkt werden.

Herausforderungen

> Niedrigschwelligkeit von verbotenen Inhalten
> Erstellung von jugendgefährdenden Inhalten durch Jugendliche

Umgang mit den Herausforderungen

> Anbieter sollen ab einer bestimmten Größe Vorsorgemaßnahmen treffen (z.B.: Meldebuttons)
> Aufsicht und Förderung durch Bundeszentralen geboten
> Institutionen befassen sich mit dem Jugendschutz
> Neue Faktoren werden berücksichtigt bei der Altersfreigabe für Spiele

Wenn Kinder in ihrer Mediennutzung auffällig werden

> Fachberatungsstellen aufsuchen (z.B. Landesstellen für Jugendschutz) – Beratung anfordern
> Mit anderen Eltern in Kontakt treten – Regeln bestimmen / sich austauschen

Weiterführende Informationen bietet z.B:
der Gefährungsatlas der Bundeszentrale für Kinder- und Jugendmedienschutz:
Weitere Informationen QR-Code 33

Handlungsbedarf

TEILHABE
> geschützte Räume bieten
> sich ausprobieren
> Beteiligung ermöglichen
> Verantwortung übernehmen

BEFÄHIGUNG
> Medienkompetenz
> digitale Bildung
> Eltern stärken
> Kultur der Mediennutzung entwickeln

SCHUTZ
> Regulierung - Selbstregulierung
> Anbieterverantwortung
> Selbstkontrolle
> Aufsicht
> Selbstschutz ermöglichen

Neuheiten im Jugendschutzgesetz

> Die Pflicht zur Alterskennzeichnung von Film- und Spielplattformen

> Der Schutz der persönlichen Integrität

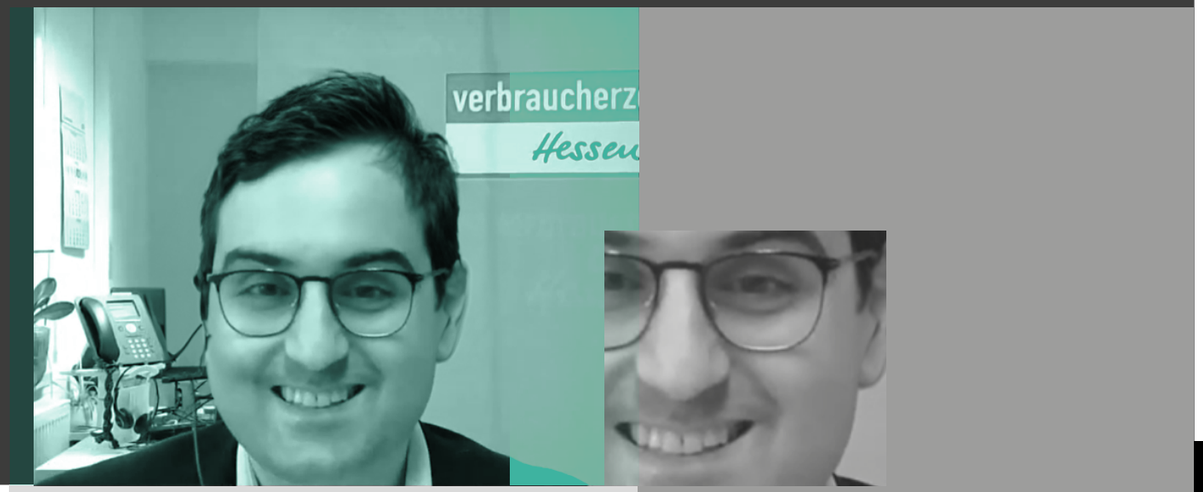
> Die Förderung der Orientierung für Kinder, Jugendliche, sorgeberechtigte Personen und pädagogische Fachkräfte bei der Mediennutzung und -erziehung

> Die Aufführung von Deskriptoren

> Die Festschreibung von einer Bundeszentrale für Kinder- und Jugendmedienschutz

> Die Parental Guidance-Regelung und Ausnahmeregelung beim Einverständnis der Sorgeberechtigten

verbraucherschutz online - was sind rechte und pflichten der verbraucher:innen?



Selahattin Beser,
Referent Recht, Verbraucherzentrale Hessen e.V.

Im Folgenden werden alle wichtigen Fragen rund um Online-Vertragsschluss, Rechte von Verbraucher:innen bei Onlinekäufen, Risiken durch kriminelle Anbieter, die Besonderheiten von Vergleichsportalen, Kriterien von Gütesiegeln und Verbraucherschutz in digitalen Räumen erörtert.

Wann entsteht aus juristischer Sicht ein Vertrag?

Ein Vertrag entsteht durch zwei übereinstimmende Willenserklärungen in Form von Angebot und Annahme. In einem Geschäft entsteht aus juristischer Sicht ein Angebot dann, wenn ein Kunde oder eine Kundin eine Ware annimmt und an die Kasse geht, um sie zu bezahlen. Der Verkäufer oder die Verkäuferin nimmt dieses Angebot an. So entsteht ein *Vertragsschluss.* Der Vertragsschluss ist besonders wichtig für Leistungspflichten, wie z.B. die **Schadensersatzansprüche.** Verträge können sowohl schriftlich wie mündlich abgeschlossen werden. Sie können ebenfalls durch konkludentes Verhalten geschlossen werden. Durch Schweigen jedoch kann kein Vertrag entstehen.

Vertragsschluss online

Möchte man Einkäufe in Online-Shops tätigen, so handelt es sich hier, ebenso wie in Offline-Geschäften nicht um Angebote, sondern um die sogenannten **invitatio ad offerendum.** Aus dem Lateinischen übersetzt bedeutet es so viel wie, der Verkäufer oder die Verkäuferin fordert dazu auf, ein Angebot abzugeben. Ist das Angebot eingegangen, so kann der Verkäufer oder die Verkäuferin es annehmen und ein Kaufvertrag kommt zustande. Annahme der Bestellung erfolgt erst mit Versendung der Ware.

Im Falle einer Vorzahlung kommt der Vertrag durch die Zahlungsaufforderung z.B. durch eine E-Mail zustande. Bei einer PayPal-Zahlung wird der Vertrag durch die Weiterleitung auf die Zahlungsseite abgeschlossen. Zu diesem Zeitpunkt entstehen bestimmte Rechte und Pflichten.

Anbieter:innen müssen Käufer und Käuferinnen über Vertragsbestandteile informieren. Besonders wichtig ist die Beschriftung des Kauf-Buttons. Dieser muss mit einer eindeutigen Beschriftung versehen werden, wie z.B.: „zahlungspflichtig bestellen". Ein einfaches „bestellen" als Beschriftung ist nicht ausreichend.

Die Aufschrift dient zur Warnung des Verbrauchers oder der Verbraucherin. Diese müssen merken, dass wenn sie auf diesen Button klicken, sie ein Angebot abgeben, das sie zur Zahlung des Kaufpreises verpflichtet.

QR-Code 34
QR-Code 35

Widerruf

Ein **Widerrufsrecht** ist nur gegeben, wenn ein Kaufvertrag bei **Fernabsatzgeschäften** zustande gekommen ist. Zu Fernabsatz zählen Online-Geschäfte oder Einkäufe per Brief, E-Mail oder durch Bestellkarten bei Werbeprospekten. Die **Widerrufsfrist** gilt 14 Tage nach Erhalt einer Ware. Der Widerruf kann mündlich, schriftlich, telefonisch, per E-Mail oder per Fax erklärt werden. Empfohlen wird ein schriftlicher Widerruf mit einer Kopie zu Beweiszwecken, falls der Widerruf nicht beim Verkäufer oder der Verkäuferin ankommen sollte. In diesem Fall muss der Kunde oder die Kundin den Widerruf nachweisen. Andernfalls wird er oder sie zur Einhaltung des Vertrages aufgefordert. Hierbei besteht das Kündigungsrecht, bei welchem Schadensersatz geleistet werden muss.

> Bei verderblicher Ware, Hygieneartikeln oder Ware, die nach wenigen Tagen nicht mehr zu gebrauchen ist, gilt das Widerrufsrecht nicht.

> Bei Verträgen mit spezifischen Terminen (z.B. Konzerten) oder einem spezifischen Zeitraum (z.B. Reisen) besteht ebenfalls kein Widerrufsrecht.

> Bei Käufen im Handel gilt kein Widerrufsrecht. Es kann vom **Gewährleistungsrecht** Gebrauch gemacht werden oder aus Kulanz eine Ware umgetauscht oder zurückgenommen werden.

QR-Code 36
QR-Code 37
QR-Code 38

verbraucherzentrale Hessen

Was passiert, wenn man etwas bestellt und die Ware nicht empfangen kann?
> Empfangsvertreter:innen können die Ware annehmen
> Erst nach Erhalt der Ware beginnt die Widerrufsfrist (bei Briefen kann es sich unterscheiden)

Was passiert, wenn man wegen einer Sprachbarriere einen unerwünschten Vertrag abgeschlossen hat?
> In den meisten Fällen ist ein Vertrag trotzdem geltend. Aus Kulanz kann er aufgelöst werden
> Es ist empfehlenswert nichts zu unterschreiben bei Verständnisschwierigkeiten

Fake Shops
Zu Fake Shops gehören gefälschte Internetseiten, Internetseiten, auf welchen gefälschte Ware angeboten wird oder die angebotene Ware nicht geliefert wird.
Meist werden Kund:innen durch Social Media oder durch andere Seiten oder Plattformen durch verlockende Angebote auf Fake Shops geleitet.

Wie erkennt man Fake Shops?
> Auffällige URL („https“ geht nicht dem Seitennamen vor)
> Nur Vorkasse bei Zahlungsmethoden
> Rechtschreibfehler bei Geschäftsbedingungen oder AGBs
> Kein Impressum
> Gefälschtes Impressum (Beim Handelsregister oder auf bundesanzeiger.de kann man prüfen, ob ein Geschäft existiert)
> Gefälschte Gütesiegel, wie z.B.: 100% Premiummarke

Wie erkennt man echte Gütesiegel?
Beim Führen des Cursors auf das Gütesiegel, erscheint ein Link, welcher auf die Seite von Trusted Shops weiterleitet, wo aufgeführt wird, dass ein Shop zertifiziert ist. Wird man auf eine andere Seite weitergeleitet, so ist es ein Zeichen dafür, dass das Siegel gefälscht ist.

Welche Gütesiegel gibt es?
> Trusted Shop Qualitätssiegel zertifiziert Händler, Reisebüros und weiteren Onlinedienste. Sie unterlaufen einer regelmäßigen finanziellen, technischen und organisatorischen Prüfung.
> EHI Siegel prüft, inwieweit der Datenschutz verbraucherfreundlich ist & ob Datenschutzbestimmungen und gesetzliche Informationspflichten eingehalten werden.
> IPS Siegel ist ein Qualitätssiegel, dass den Datenschutz kontrolliert.

QR-Code 39
QR-Code 40

Was kann man im Ernstfall tun?
> Strafanzeige bei der Polizei einreichen
> Bildschirmfotos von der Webseite und von den E-Mails des Anbieters erstellen
> Bank auffordern die Zahlung rückgängig zu machen

Phishing
Beim Phishing geht es darum, dass private Daten von Menschen abgegriffen werden und sie dadurch hintergangen werden. Hierbei handelt es sich um Passwörter, Kreditkartendaten oder andere vertrauliche Informationen. Benutzer:innen werden durch E-Mails kontaktiert und aufgefordert Links anzuklicken oder Formulare auszufüllen, weil z.B. sonst gedroht wird, ihr Amazon-Konto zu sperren. In der E-Mail wird zumeist eine Dringlichkeit vermittelt, die Angst und Druck verbreiten soll. Des Weiteren wird man nicht mit Namen angesprochen und aufgefordert Dateien zu öffnen, die Viren enthalten. Durch das Prüfen des E-Mail Headers (Kopfzeile) und der IP-Adresse kann erkannt werden, wer sich hinter der E-Mail verbirgt.

QR-Code 41

Was kann man im Ernstfall tun?
> Strafanzeige bei der Polizei einreichen
> Bildschirmfotos von der Webseite und von den E-Mails des Anbieters erstellen

Vergleichsportale
Vergleichsportale überprüfen und vergleichen Angebote. So können sich Nutzer:innen über Ticketpreise z.B. bei Flugtickets oder über Versicherungen informieren. Check24 ist eines der bekanntesten Vergleichsportale.
Es besteht eine Möglichkeit durch das Vergleichsportal einen Vertragsabschluss zu tätigen. Hierbei dient das Vergleichsportal als Vermittler, welcher eine Provision von den Anbietern bekommt. Der Vertrag wird zwischen Nutzer:in und Anbieter geschlossen.

Welche Tricks werden angewandt?
> Falsche Gütesiegel
> Tiefpreisgarantie (Bedingungen unter Vorbehalt)
> Gefälschte Begrenztheit und Exklusivität der Ware
> Gefälschte Bewertungen
> Manipuliertes Ranking der Ergebnisse

Änderungen der rechtlichen Grundlage für Vergleichsportale - Neue Transparenzregeln:
> Hauptparameter, die für das Ranking zuständig sind, sollen auf der Benutzeroberfläche dargestellt werden
> Marktplatzbetreiber müssen deutlich machen, ob es sich bei dem Verkäufer oder der Verkäuferin um ein Unternehmen oder eine Privatperson handelt (Wichtig u.A. für das Widerrufsrecht)
> **Weitere Informationen** QR-Code 42

Zusammen-fassung

Das fortschreitende Verschmelzen digitaler und analoger Lebenswelten steigert die Notwendigkeit, Menschen - insbesondere Gruppen, deren Teilhabe an gesellschaftlichen Prozessen ohnehin eingeschränkt ist - für die Chancen und Risiken dieser Räume gleichermaßen zu sensibilisieren. Mit dieser Broschüre sollen Kenntnisse über die eigenen Rechte, den Schutz vor Missbrauch und die Handhabe mit Daten in Online-Räumen vermittelt und somit auf niedrigschwelliger Ebene Medienkompetenz gefördert werden.

Jegliches Verhalten im Netz hinterlässt einen sogenannten “digitalen Abdruck” der Nutzer:innen, den Plattformen für verschiedene Zweck verwenden können. Konzerne wie Amazon, Netflix oder Facebook können Informationen über Personen anhand ihrer Datenspur sammeln und dieses Wissen für ihre Gewinnmaximierung nutzen. Was viele nicht wissen: Im Grunde können alle Nutzer:innen auf Basis einer der dafür geltenden gesetzlichen Grundlage die eigene Datenspur herausfinden. Das sieht die EU DSGVO vor. Die Netzaktivistin und Politikerin Katharina Nocun hat einen Selbstversuch gemacht und darüber ein Buch geschrieben.

Allein in Deutschland sind schätzungsweise zwei Millionen Schüler und Schülerinnen von Cybermobbing betroffen.

Lukas Pohland war einer von ihnen und hat beschlossen, mit der Gründung seines Vereins für Betroffene aktiv zu werden. Er beschreibt, wie man mit Cybermobbing umgehen kann, welche Lösungsansätze es gibt, was Betroffene und ihr Umfeld dagegen tun können und wie Täter:innen bestraft werden können.

Durch den Digital Services Act sollen auf gesetzlicher Ebene Problematiken im Internet adressiert und EU-übergreifend geregelt werden. Dr. Daniel Holznagel war bereits in der Vergangenheit an der Entwicklung von Gesetzen beteiligt, die die Regulierung von Online-Räumen sicherstellen sollen und gibt Einblick in Regulierungsmöglichkeiten, die durch den DSA gegeben werden. Auch aus der Entstehung des Digital Services Act geht hervor, dass Nutzer:innen im Netz bislang nicht hinreichend von ihrem Recht Gebrauch machen, auf ihre eigenen Daten zuzugreifen oder gegen eine missbräuchliche Nutzung von Plattformen rechtlich vorzugehen.

Die informierte und bewusste Nutzung digitaler Medien kann insbesondere für vulnerable und marginalisierte Gruppen eine Herausforderung darstellen. Gleichzeitig kann das sichere Zurechtfinden in digitalen Lebenswelten zukünftig auch für diese Gruppen Entlastungspotenziale bieten. Auch jugendliche Lebenswelten spielen sich zunehmend in Online-Räumen ab, wie die regelmäßigen Erhebungen durch die JIM- und KIM-Studien zeigen.

Der rasante Medienwandel der vergangenen Jahre stellt auch eine Herausforderung für den Kinder- und Jugendschutz dar, der die Aufgabe hat, junge Menschen einerseits vor potenziell gefährdenden Inhalten zu schützen und sie und ihr soziales Umfeld gleichzeitig zu einer mündigen Nutzung neuer Medien zu befähigen.

Auch auf Einkäufe in digitalen Räumen wirken sich Fragen nach dem Schutz und den Rechten von Endverbraucher:innen aus. Darauf hat sich der Verbraucherschutz in den vergangenen Jahren auch spezialisiert. Das Grundwissen zu unterschiedlichen Aspekten der Netzpolitik und des Verbraucherschutzes bietet eine erste Orientierung in diesem sich stetig weiterentwickelnden Bereich.

qr-code-verzeichnis

1
Artikel 15 (S. 12)

2
Big Data (S. 13)

3
Click Steam (S. 14)

4
IP-Adresse (S. 14)

5
VPN (S. 14)

6
Netflix (S. 14)

7
Profiling (S. 15)

8
Snowden-Skandal (S. 15)

9
Microtargeting (S. 15)

10
Data-Literacy (S. 16)

11 Cybermobbing-hilfe.de (S. 20)

12 Cherry Picking (S. 22)

13
Filesharing (S. 22)

14
Urheberrecht (S. 22)

15
Hate Speech (S. 22)

16
Status DSA (S. 25)

17
Status DSA (S. 27)

18
DigBitS (S. 29)

19
Klicksafe (S. 30)

20
Digitaler Engel (S. 30)

21 Digital-Kompass (S. 30)

22
PolisiN (S. 30)

23 Digital-führerschein (S. 30)

24
FSK (S. 32)

25
USK (S. 32)

26
JIM-Studie (S. 32)

27
KIM-Studie (S. 32)

28
Fake News (S. 33)

29
Sexting (S. 34)

30 Cyber-Grooming (S. 34)

31
Cybermobbing (S. 34)

32
Smart Home (S. 34)

33 Parental Guidance (S. 35)

34 Schadens-ersatzanspruch (S.38)

35 Invitatio ad Offerendum(S. 38)

quellen

1 EU Datenschutzgrundverordnung Artikel 15 (S. 12)
https://dsgvo-gesetz.de/art-15-dsgvo/

2 Big Data (S. 13)
https://www.oracle.com/de/big-data/what-is-big-data/

3 Click Stream (S. 14)
https://www.fachmedien.ch/component/seoglossary/1-glossar/click-stream.html

4 IP-Addresse (S. 14)
https://www.avast.com/de-de/c-what-is-an-ip-address

5 VPN (S. 14)
https://www.computerweekly.com/de/definition/Virtuelles-Privates-Netzwerk-Virtual-Private-Network-VPN

6 Netflix (S. 14)
https://praxistipps.chip.de/was-ist-netflix-einfach-erklaert_41510

7 Profiling (S. 15)
https://persomatch.de/hr-lexikon/profiling/

8 Snowden-Skandal (S. 15)
https://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal

9 Microtargeting (S. 15)
https://www.marconomy.de/microtargeting-definitioneinsatz-und-beispiele-a-739666/

10 Data-Literacy (S. 16)
https://www.bigdata-insider.de/was-ist-data-literacy-a-823501/

11 Cybermobbing-hilfe.de (S. 20)
https://www.cybermobbing-hilfe.de

12 Cherry Picking (S. 22)
https://lexikon.stangl.eu/28950/cherry-picking

13 Filesharing (S. 22)
https://www.ionos.de/digitalguide/server/knowhow/was-ist-filesharing/

14 Urheberrecht (S. 22)
https://www.urheberrecht.de/

15 Hate Speech (S. 22)
https://www.amadeu-antonio-stiftung.de/digitale-zivilgesellschaft/was-ist-hate-speech/

16 Status DSA (S. 25)
https://hateaid.org/dsa-user-guide/

17 Status DSA (S. 27)
https://digital-strategy.ec.europa.eu/de/policies/safer-online

18 DigiBitS (S. 29)
https://www.digibits.de/

19 Klicksafe (S. 30)
https://www.klicksafe.de/

20 Digitaler Engel (S. 30)
https://www.digitaler-engel.org/

21 Digital-Kompass (S. 30)
https://www.digital-kompass.de/

22 PolisiN (S. 30)
https://www.polisin.de/

23 Digitalführerschein (S. 30)
https://xn--dif-joa.de/

24 FSK (S. 31)
https://www.schau-hin.info/sicherheit-risiken/fsk-alterskennzeichen-fuer-film#:~:text=Die%20Freiwillige%20Selbstkontrolle%20der%20Filmwirtschaft%20(FSK)%20bestimmt%20die%20jeweilige%20Altersuntergrenze,f%C3%BCr%20Kinder%20und%20Jugendliche%20einstuft.

25 USK (S. 31)
https://usk.de/die-usk/arbeit-der-usk/wer-ist-die-usk/

26 JIM-Studie (S. 32)
https://www.mpfs.de/studien/jim-studie/2022/

quellen

27 KIM-Studie (S. 32)
https://www.mpfs.de/fileadmin/files/Studien/KIM/2020/KIM-Studie2020_WEB_final.pdf

28 Fake News (S. 33)
https://www.lmz-bw.de/medienbildung/themen-von-f-bis-z/hatespeech-und-fake-news/fake-news/was-sind-fake-news

29 Sexting (S. 34)
https://www.klicksafe.de/sexting

30 Cyber Grooming (S. 34)
https://www.klicksafe.de/cybergrooming

31 Cybermobbing (S. 34)
https://www.bmfsfj.de/bmfsfj/themen/kinder-und-jugend/medienkompetenz/was-ist-cybermobbing--86484#:~:text=Unter%20Cyberbullying%20oder%20Cybermobbing%20versteht,%2C%20Foren%2C%20Chats%20und%20Communities.

32 Smart Home (S. 34)
https://www.bosch-smarthome.com/at/de/smart-home-erklaert/#:~:text=Unter%20dem%20Begriff%20Smart%20Home,im%20intelligenten%20Zusammenspiel%20der%20Ger%C3%A4te.

33 Parental Guidance-Regelung (S. 35)
https://www.moviepilot.de/news/so-funktioniert-die-pg-regelung-der-elternbegleitung-1108010

34 Schadensersatzanspruch (S. 38)
https://www.procontra-online.de/lexikon/schadensersatzanspruch

35 Invitatio ad Offerendum (S. 38)
https://www.juraforum.de/lexikon/invitatio-ad-offerendum

36 Widerrufsrecht (S. 38)
https://www.procontra-online.de/lexikon/widerrufsrecht

37 Fernabsatzgeschäft (S. 38)
https://www.juraforum.de/lexikon/fernabsatzgeschaeft

38 Gewährleistungsrecht (S. 38)
https://www.studysmarter.de/schule/wirtschaft/rechtslehre/gewaehrleistung/

39 EHI (S. 39)
https://ehi-siegel.de/

40 IPS (S. 39)
https://www.datenschutz-cert.de/leistungen/ips-internet-privacy-standards

41 Phishing (S. 40)
https://wirtschaftslexikon.gabler.de/definition/phishing-53396

42 Transparenzregeln (S. 40)
https://www.verbraucherzentrale-hessen.de/pressemeldungen/vertraege-reklamation/mehr-transparenz-bei-einkauf-und-vertragsschluss-im-netz-73715

raum für notizen