Hochschule Düsseldorf
University of Applied Sciences

Fachbereich Medien
Faculty of Media

Datenbanken und E-Business
Databases and E-Business

Prof. Dr.-Ing. Thomas C. Rakow
thomas.rakow@hs-duesseldorf.de
info@rakow.biz
dbe.medien.hs-duesseldorf.de

Problemfälle des E-Business – Tracking und Anonymität

Arbeitspapier des Lehrgebiets
Datenbanken und E-Business
No. 1/2024

herausgegeben von

Thomas C. Rakow

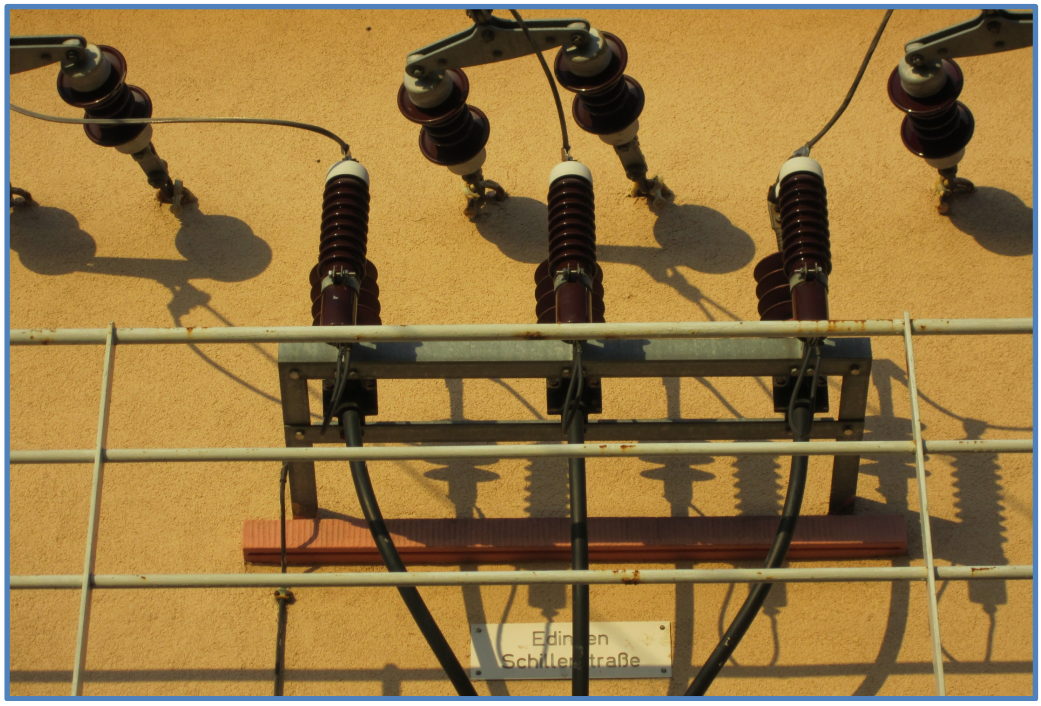


Bild: Kraftwerkanschluss.
© Thomas Rakow.

© Die Autoren 2024
Open Access: Dieser Beitrag wird unter der Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz (https://creativecommons.org/licenses/by-sa/4.0/deed.de) veröffentlicht. Ausgenommen von der Lizenzierung sind anderweitig gekennzeichnete Inhalte sowie die verwendeten Logos der beteiligten Institutionen.

Zum Geleit

Im E-Business werden die automatisierbaren Geschäftsprozesse von Unternehmen zusammengefasst. Im Seminar der Veranstaltung zu diesem Thema sollten die Teilnehmer zu einer vorgegebenen Fragestellung, die erfahrungsgemäß hohe Anforderungen an die technische und organisatorische Umsetzung einer Beantwortung erfordert, eine Ausarbeitung aufgrund einer Recherche wissenschaftlicher und technischer Veröffentlichungen sowie eine Website im WordPress CMS nach vorgegebenem Muster erstellen. Zu zwei Fragestellungen sind in diesem Arbeitspapier die Ausarbeitungen enthalten:

- Wer verfolgt mich? – Die Krux mit dem Tracking
- Wie gut, dass keiner weiß – Anonymität im Web (inklusive Dark Net)

Auf der Website sollten max. 3 Webseiten für einen interessierten Betrachter erstellt werden. Der Betrachter sollte interaktiv mit der Webseite bzw. den Webseiten agieren können. In einem Making-of auf einer weiteren Seite sollten Konzept, Design, Entwicklung und Test der Webseiten(n) dokumentiert werden. Zur Ergänzung der Ausarbeitung werden die Webseiten als Ausdruck angefügt, auch wenn sie hier nicht die interaktiven Möglichkeiten zeigen.

Die Studierenden haben diese Arbeiten in den Studiengängen B.Sc. Medieninformatik bzw. M.Sc. Medieninformatik der Hochschule Düsseldorf als Prüfungsleistung erstellt. Ich danke Till Büge, Julian Fitzen, Marcel Joschko, Hasan Kahraman, Sven Schoop und Luca Selinski für ihre Beteiligung an diesem Arbeitspapier meines Lehrgebietes.

Düsseldorf, 08.05.2024 *Professor Dr.-Ing. Thomas C. Rakow*

Inhaltsverzeichnis des Arbeitspapiers

Hochschule Düsseldorf
University of Applied Sciences

Fachbereich Medien
Faculty of Media

Datenbanken und E-Business
Databases and E-Business

Seminararbeit

E-Business

Wintersemester 2023/24

Wer verfolgt mich? Die Krux mit dem Tracking

Julian Fitzen
Marcel Joschko
Hasan Kahraman

9. April 2024

Inhaltsverzeichnis

Metadaten

Deutsche Kurzfassung

Diese Seminararbeit beleuchtet das Thema Online-Tracking und seine Auswirkungen auf die Privatsphäre und den Datenschutz. Es wird untersucht, wer mit welchen Zielen digitale Spuren hinterlässt, insbesondere im E-Commerce. Die Rolle von Unternehmen im Tracking-Prozess und der Einsatz verschiedener Technologien wie Cookies und Cross-Device-Tracking werden diskutiert. Darüber hinaus werden Handlungsoptionen für Nutzer und ethische Aspekte, einschließlich der Einhaltung der DSGVO, diskutiert. Ziel der Arbeit ist es, ein Bewusstsein für die Komplexität und die ethischen Herausforderungen des Trackings zu schaffen und Wege zum Schutz der Nutzerdaten aufzuzeigen.

Englische Kurzfassung

This paper examines the issue of online tracking and its implications for privacy and data protection. It examines who leaves digital traces and for what purposes, particularly in e-commerce. It discusses the role of companies in the tracking process and the use of different technologies such as cookies and cross-device tracking. In addition, options for users and ethical aspects, including compliance with the GDPR, will be discussed. The aim of the work is to raise awareness of the complexity and ethical challenges of tracking and to show ways to protect user data.

Stichworte

Online-Tracking; Datenschutz; Privatsphäre; E-Commerce; Tracking-Technologien; Nutzerdatensicherheit; Ethik im Digitalzeitalter; DSGVO; Datenverarbeitung; Digitale Privatsphäre; Cookies

Anzahl der Wörter

Die Seminararbeit umfasst 4108 Wörter. Es wurden nur die nummerierten Kapitel berücksichtigt.

1 Einleitung

Die zentrale Frage dieser Seminararbeit lautet: "Wer verfolgt mich? - Die Krux mit dem Tracking". Die Entwicklung des Trackings begann in den 1940er Jahren mit der Segmentierung von Personen für Kreditrisiken. Nach der Einführung des World Wide Web im Jahr 1991 wurde mit der Entwicklung des HTTP-Cookies ein bedeutender Fortschritt erzielt. Diese Technologie führte zu personalisierter Online-Werbung, die sich in den folgenden Jahren weiterentwickelte. Ab 2008 begann das Tracking des Nutzerverhaltens, insbesondere im Zusammenhang mit sozialen Medien. [Kan21] In der heutigen Welt, in der das Internet eine unersetzliche Rolle in unserem Alltag spielt, wächst mit unserer zunehmenden Abhängigkeit von Technologien und digitalen Plattformen auch die Sorge um den Schutz unserer Privatsphäre und die Sicherheit unserer Daten. Diese Entwicklung wirft grundlegende Fragen auf: Wer überwacht unsere Online-Aktivitäten, insbesondere im Zusammenhang mit E-Commerce? Was sind die Absichten dieser Akteure? Diese Arbeit geht diesen Fragen nach und beleuchtet die komplexen Dynamiken und Konsequenzen des Online-Tracking in unserer heutigen digitalen Welt.

Kapitel 2 untersucht die Rolle profitorientierter Unternehmen und deren Ziele im Kontext des Online-Tracking. Es wird untersucht, wie diese Unternehmen Daten sammeln und nutzen, um ihre Dienstleistungen und Produkte zu optimieren.

In Kapitel 3 werden die verschiedenen Technologien beschrieben, die beim Tracking zum Einsatz kommen. Dazu gehören Cookies, Tracking-Pixel, Event Tracking, Ultrasound Cross-Device Tracking und Tools zur Verarbeitung der Daten.

Kapitel 4 zeigt Handlungsoptionen für Nutzer auf. Dazu gehören die Darstellung der Vorteile von Webtracking aus Nutzersicht im E-Commerce, die Nutzung von kostenlosen State-of-the-Art-Produkten und Maßnahmen zur Stärkung der Nutzerdatensicherheit.

Kapitel 5 konzentriert sich auf die ethischen Aspekte des Trackings. Der Datenschutz nach der DSGVO, die Verarbeitung personenbezogener Daten und die Notwendigkeit von Einwilligungen und Datenschutzerklärungen werden diskutiert.

Abschließend fasst Kapitel 6 die wichtigsten Erkenntnisse zusammen und Kapitel 7 zeigt mögliche zukünftige Entwicklungen und Herausforderungen im Bereich Online-Tracking und Datenschutz auf.

Ziel dieser Arbeit ist es, ein tieferes Verständnis für die Komplexität und die ethischen Implikationen des Trackings in unserem digitalen Alltag zu entwickeln und aufzuzeigen, wie Nutzer ihre Daten schützen können.

2 Wer verfolgt mich?

Im digitalen Zeitalter ist das Internet aus unserem Leben nicht mehr wegzudenken. Die zunehmende Abhängigkeit von der Technologie und dem Cyberspace hat jedoch auch zu Bedenken hinsichtlich des Schutzes der Privatsphäre und der Datensicherheit

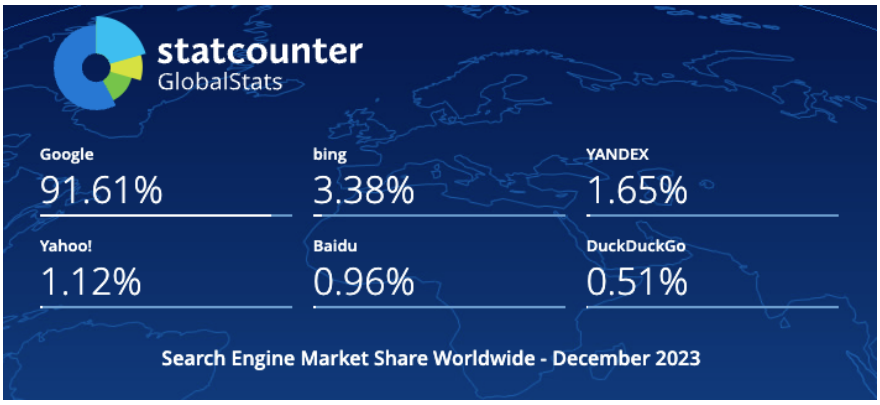


Abbildung 1: Marktanteil der Suchmaschinen weltweit von Dezember 2022 bis Dezember 2023 [Sta23a]

geführt. In diesem Kapitel geht es darum, wer uns online und im E-Commerce verfolgt und aus welchem Grund.

2.1 Profitorientierte Unternehmen

In der Welt der Technologie wird oft von den fünf großen Technologieunternehmen gesprochen: Alphabet (Google), Amazon, Meta, Apple und Microsoft. Amazon wird oft zu den *Big Five* gezählt, obwohl es kein reines Technologieunternehmen ist und sein Kerngeschäft im E-Commerce liegt. Diese Unternehmen haben mit ihren Produkten nicht nur eine Quasi-Monopolstellung in der Technologiebranche, sondern generieren im Vergleich zu anderen Nicht-Technologieunternehmen auch enorme Umsätze. Zusammen haben die *Big Five* Technologieunternehmen im Jahr 2023 einen Umsatz von mehr als 1.500 Milliarden US-Dollar erwirtschaftet. [Sta23b; Ana23] Darüber hinaus waren vier der fünf größten Technologieunternehmen maßgeblich für den Anstieg des S&P 500 verantwortlich, einem Aktienindex, der die Performance der 500 größten US-Unternehmen am Aktienmarkt abbildet. [Phi23]

Die Monopolstellung dieser Unternehmen ist bei einigen Produkten so dominant, dass sie im Fall der Suchmaschine Google weltweit mehr als 90 % aller Desktop-, Tablet- und Mobilgeräte abdeckt. In Abbildung 1 ist die weltweite Aufteilung von Suchmaschinennutzung dargestellt. Die Statistik bezieht sich auf den Zeitraum von Dezember 2022 bis Dezember 2023. [Sta23a]

Diese enorme Marktdominanz kann sehr gefährlich sein, da die Nutzer von Suchmaschinen keine gleichwertige Alternative zur Auswahl haben und Google somit der einzige ist, der Zugang zu den Nutzerdaten hat. Einerseits kann Google so seine Position halten, andererseits können andere, weniger bekannte Suchmaschinen wie DuckDuckGo nicht in gleichem Maße am Markt teilnehmen.

Die *Big Five* Technologieunternehmen sind jedoch nicht die einzigen profitorientierten Unternehmen auf dem Markt. Viele große Unternehmen wie Spotify und Netflix verfolgen die Daten ihrer Nutzer. [Fit20; Gar+18] Beispielsweise nutzt Netflix die Daten um bessere Film-Empfehlungen machen zu können.

2.2 Ziele der Verfolger

Eines der Hauptziele des Trackings von Nutzerdaten ist die Bereitstellung eines hochwertigen Nutzererlebnisses. Durch das Sammeln von Daten über die Interessen und das Verhalten der Nutzer können Unternehmen ihre Dienstleistungen anpassen und das Nutzererlebnis verbessern. Personalisierte Empfehlungen, zielgerichtete Werbung und spezielle Funktionen können dazu beitragen, die Zufriedenheit der Nutzer zu erhöhen. Es ist jedoch wichtig, dass diese Personalisierung transparent ist und von den Nutzern verstanden wird. So sollten die Aktivitäten der Nutzer nur mit ihrer ausdrücklichen Zustimmung verfolgt werden.

Das Tracking von Nutzerdaten dient auch der Generierung von Einnahmen. Durch das Sammeln großer Datenmengen erhalten Unternehmen wertvolle Ressourcen, die sie nutzen können. Diese Daten können durch gezielte Werbung und Partnerschaften mit anderen Unternehmen zu Geld gemacht werden. Durch die Nutzung von Nutzerdaten können Unternehmen in Innovationen investieren, um sicherzustellen, dass ihre kostenlosen Dienste rentabel sind.

Eine der wichtigsten Methoden, die diese Unternehmen anwenden, um das Verhalten und die Vorlieben der Nutzer zu ermitteln, ist *Predictive Analytics*. Sie nutzen große Datenmengen und setzen intelligente Algorithmen und maschinelles Lernen ein, um das Verhalten und die Vorlieben der Nutzer vorherzusagen. Auf diese Weise können den Nutzern realistischere Empfehlungen gegeben werden, z. B. personalisierte Produktempfehlungen oder zielgerichtete Werbung. [Kol19]

3 Verwendete Technologien im Tracking

In diesem Kapitel werden verschiedene Technologien untersucht, die im Tracking verwendet werden. Zunächst werden Cookies und ihre verschiedenen Anwendungsformen im Webtracking erläutert, gefolgt von der Beschreibung von Tracking-Pixeln und ihrer Funktionsweise. Anschließend wird Event Tracking vorgestellt, eine Methode zur Analyse von Nutzeraktionen auf Webseiten. Ultrasound-Cross-Device-Tracking wird als fortschrittliche Technologie zur geräteübergreifenden Datenerfassung diskutiert. Abschließend werden Tools zur Verarbeitung der gesammelten Daten vorgestellt. Dabei werden sowohl kommerzielle als auch Open-Source-Optionen berücksichtigt.

3.1 Cookies

Cookies sind Textdateien, die von Website-Betreibern genutzt werden, um Informationen über Besucher zu speichern. Dabei wird eine Textdatei mit einer eindeutigen Kennung erstellt, die zur Identifizierung eines Benutzers verwendet wird.

Im Gegensatz zu anderen Webseitenbetreibern verwendet Facebook Cookies nicht ausschließlich für die eigene Webseite, sondern auch für das gesamte Netzwerk von Webseitendiensten und Einbettungen. Es ist möglich, dass Facebook Cookies auch nach dem Ausloggen eines Nutzers weiterhin verwendet, um den Nutzer auf Webseiten, die

Facebook-Code oder -Einbettungen verwenden, zu verfolgen. Facebook weist den Vorwurf zurück und argumentiert, dass die angesprochenen Cookies nach dem Ausloggen nur zur Account-Sicherheit und Personalisierung verwendet werden. [Pro11]

Third-Party-Cookies werden meist von Werbetreibenden eingesetzt. Diese können Nutzer wie bereits beschrieben über mehrere Seiten hinweg verfolgen und Präferenzen für Produkte oder Werbung erstellen. Die dadurch gesammelten Daten liegen bei einem zentralen Dienst wie beispielsweise Google. Laut einer Umfrage verfügen 48 % der deutschen Unternehmen über Third-Party-Cookies und die damit verbundenen Daten. [Axc23]

3.2 Tracking-Pixel

Tracking-Pixel oder Zählpixel sind unsichtbare 1x1-Grafiken, die in der Regel in E-Mails oder HTML-Webseiten eingebettet sind. Sie erfassen in der Regel die IP-Adresse, den Browser, das Betriebssystem oder zählen einfach, wie oft ein Artikel aufgerufen wurde.

Durch die Erfassung einer IP-Adresse können ohne das Wissen oder die Zustimmung des Nutzers geo-sensible Daten an Dritte weitergegeben werden. Im Gegensatz zu Cookies ist für Tracking-Pixel keine explizite Zustimmung des Nutzers erforderlich, sei es freiwillig oder unfreiwillig. Dies ist besonders problematisch, wenn nicht anonymisierte Daten durch E-Mail-Tracking-Pixel erhoben werden. Darüber hinaus ist den meisten Nutzern der Umfang der Datenerhebung nicht bekannt. [Ion22; Wik23b]

Einige E-Mail-Programme bieten Schutz gegen Tracking-Pixel. Eine Möglichkeit besteht darin, keinen HTML-Code zu laden. Dadurch können auch kein JavaScript und somit keine Datenerfassung ausgeführt werden. Außerdem können externe Grafiken blockiert oder dem Mailprogramm die Internetzugriffsrechte eingeschränkt werden. [Wik23b]

3.3 Event Tracking

Hierbei handelt es sich um eine Methode, Ereignisse auf einer getrackten Webseite zu analysieren und zu verarbeiten. Die gewissen Parameter und Definition eines Events hängen gänzlich von den Bedürfnissen des Betreibenden ab. Einige Beispiele sind Seitenaufrufe, Klicks, Scroll-Verhalten, Tastatureingaben oder auch Bewegungen mit der Maus. [Ung23]

Durch eine umfassende Analyse des Nutzerverhaltens können Designentscheidungen für eine Webseite getroffen werden. Wenn eine Funktion der Webseite auffällig oft falsch verstanden wird oder ein Analyseergebnis zeigt, dass sie im Nutzungsverlauf oft nicht gefunden oder übersehen wird, kann sie durch eine neue Position, auffälligere Farben oder einen besseren Leitfaden für den Nutzer angepasst werden. Für diesen hochkomplexen Prozess werden oft A/B-Tests angewandt oder externe Tools wie Microsoft Clarity verwendet. [MSO; Ryt]

3.4 Ultrasound Cross-Device Tracking

Ultrasound Beacon Tracking ist eine Methode, mit der ein Service oder Werbetreibender die simultane Nutzung von verschiedenen elektronischen Geräten feststellen kann. Dabei wird von einer Quelle ein hochfrequentes Schallsignal (18 kHz - 20 kHz) erzeugt, welches zur Identifizierung dieser von anderen Geräten genutzt werden kann. Das menschliche Gehör kann diesen "Tag"nicht wahrnehmen, andere Geräte mit einem Mikrofon jedoch schon.

Durch die geräteübergreifende Datensammlung können Werbetreibende, die normalerweise nur begrenzte Tracking-Möglichkeiten haben, ein detailliertes Nutzerprofil erstellen und verfolgen, wie Kunden geworben werden konnten. Ein Beispiel hierfür ist ein TV-Werbespot, der einen Ultrasound-Tag einbettet. Dadurch kann ein mobiles Endgerät erkennen, ob ein Nutzer den Werbespot angesehen hat und diesen auch online präsentieren. Dadurch entsteht auch der Effekt, dass 31 % der Befragten einer Statista-Studie den Eindruck haben, dass ihr Handy bereits abgehört wurde. [Boc23] Ein Überblick über die Ergebnisse der Befragung ist in Abbildung 2 dargestellt.

Forschende haben Feldanalysen durchgeführt und herausgefunden, dass in 4 von 35 europäischen Geschäften Ultraschall-Beacons zur Standortverfolgung verwendet werden können. In derselben Studie wurden auch 223 Android-Apps entdeckt, die den Nutzer ohne Zustimmung belauschen können.

Die größte Gefahr für den Nutzer besteht darin, dass er nicht erfahren kann, ob eines oder mehrere seiner Geräte gerade diese Technologie verwenden. Es besteht die Möglichkeit, dass dem Nutzer einige Geräte zugeordnet werden können. Wenn der Nutzer auf einem Gerät besonders vorsichtig ist und darauf achtet, welche Daten er preisgibt, kann ein anderes Gerät, welches durch Cross-Device-Tracking diese Daten preisgibt, die Vorsicht zunichte machen. Die verschiedenen Anwendungen von Ultrasonic Beacon sind in Abbildung 3 dargestellt.

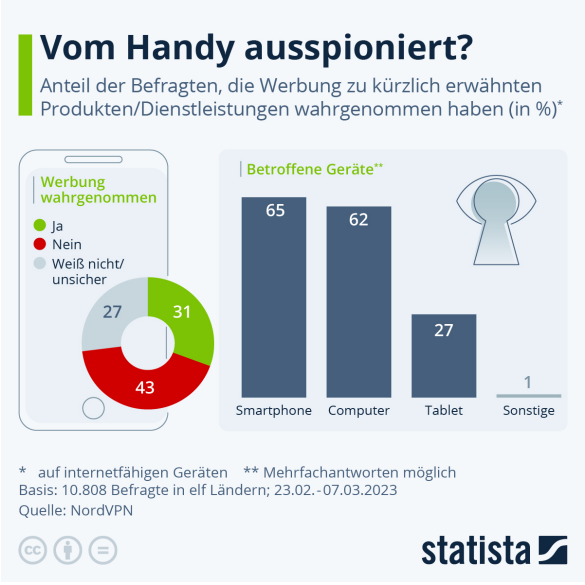


Abbildung 2: Befragung: Vom Handy ausspioniert? [Boc23]

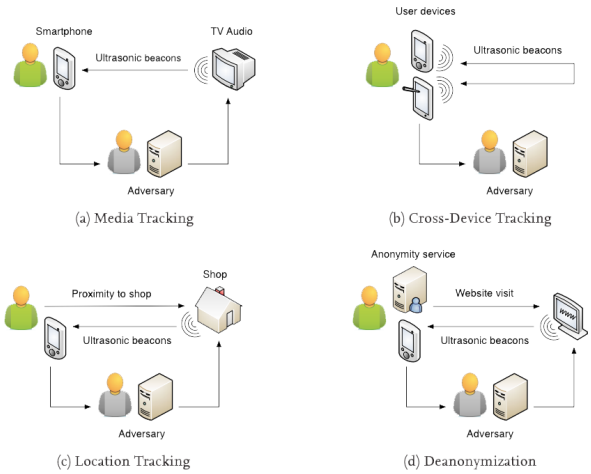


Abbildung 3: Verschiedene Arten von Ultrasonic Beacons [Arp+16]

Wenn ein Nutzer bei einer Transaktion anonym bleiben möchte, kann er dies normalerweise durch den Dezentralisierungsaspekt der Blockchain sicherstellen. Allerdings kann die Anonymität aufgehoben werden, wenn die Webseite, auf der die Transaktion stattfindet, ein Ultraschallsignal aussendet und ein identifizierbares mobiles Endgerät desselben Nutzers erkannt wird. Dieses Prinzip kann auch auf den Tor-Browser und die besuchten Webseiten angewendet werden. [Arp+16]

Forschende haben schnell auf die damit verbundene Gefahr hingewiesen. Im Jahr 2016 hat die FTC 12 Entwickler, die den Code für Ultrasound Cross Device Tracking verwenden, darauf hingewiesen, dass sie rechtswidrig handeln, wenn sie die Verbraucher nicht darüber informieren. In Deutschland ist es außerdem nicht erlaubt, Werbetechniken anzuwenden, bei denen Werbung nicht eindeutig von anderen Sendungsteilen räumlich oder akustisch abgesetzt werden kann. [Wik23a]

In der EU gilt auch die Datenschutz-Grundverodnung (DSGVO). Unternehmen, die personenbezogene Daten von EU-Bürgern erheben möchten, müssen zuvor die Zustimmung des Nutzers einholen. Es bleibt jedoch fraglich, wie viele Unternehmen oder Anwendungen dies bei einer so versteckten Tracking-Technologie tatsächlich tun.

3.5 Tools zur Verarbeitung erhobener Daten

Daten, die durch verschiedene Tracking-Methoden erhoben wurden, müssen übersichtlich und effektiv verarbeitet werden. Hierfür gibt es sowohl kommerzielle als auch Open-Source Produkte. Im Folgenden werden zwei gängige Tools verglichen und ihre Anwendungszwecke aufgeführt. Außerdem wird eine Open-Source Lösung vorgestellt.

Ein übersichtliches Tool zur Analyse des Nutzerverhaltens auf der eigenen Website. Das Tool richtet sich an Website-Betreiber, die das Verhalten der Nutzer analysieren und zur Optimierung nutzen möchten. Durch Technologien wie Heatmaps (oft geklickte Zonen oder Bereiche auf einer Webseite) oder Event-Tracking kann die Usability einer Webseite verbessert werden.

Google Ads nutzt die erhobenen Daten sogar websiteübergreifend, um personalisierte Werbung zu schalten. Dieser Service ermöglicht es Werbetreibenden, personalisierte Werbung auf ihrer eigenen Website zu schalten. Google bietet somit eine zentrale Lösung für dezentrales Werben.

Ein Kritikpunkt ist die mangelnde Transparenz bezüglich der von Google gesammelten Daten. Zudem hat Google mit seiner Suchmaschine eine Monopolstellung inne und kann Daten von einzelnen Nutzern über das gesamte Internet erheben. Im Jahr 2023 hatte Google einen geräteübergreifenden Marktanteil von 91.61 %. [Sta23a]

Eine Alternative zu den Diensten von Großkonzernen bietet der selbst gehostete Service Umami. Dieser ist Open-Source und ermöglicht es, die DSGVO-Richtlinien einzuhalten und die erhobenen Daten im Falle einer EU-Firma selbst zu hosten. Somit kann eine Firma selbst bestimmen, was mit den sensiblen Daten der Nutzenden geschieht.

4 Handlungsmöglichkeiten für den Nutzer

In diesem Kapitel werden Handlungsmöglichkeiten für Benutzer im Kontext des Web-Trackings im E-Commerce aufgezeigt. Zunächst werden die Vorteile des Web-Trackings aus Nutzersicht beleuchtet, einschließlich personalisierter Erfahrungen und optimierter Einkaufsprozesse. Anschließend wird die Nutzung kostenloser, moderner Produkte und die damit verbundenen Datenschutzbedenken diskutiert. Abschließend werden präventive Maßnahmen zur Stärkung der Sicherheit von Nutzerdaten und zum Schutz vor unerwünschtem Tracking vorgestellt.

4.1 Vorteile des Web-Trackings aus Nutzersicht im E-Commerce

Der Einsatz von Webtracking im E-Commerce kann sowohl für Shopbetreiber als auch für Kunden positive Auswirkungen haben. Laut einer Studie spricht personalisierte Produktempfehlungen und Werbung rund ein Drittel der Internetnutzer an. Die Analyse des Kauf- und Klickverhaltens kann sich zudem positiv auf das Produktangebot auswirken. [Ber18] Webtracking erleichtert die Nutzung von Online-Shops durch die Speicherung von Warenkorbinhalten, auch ohne Kundenkonto. Die Erfassung des Klick- und Kaufverhaltens kann sich preislich für den Kunden auswirken, indem Erinnerungsmails mit Rabatten den Kaufanreiz erhöhen.

Ein zentraler Vorteil des Web-Trackings im E-Commerce aus Nutzersicht besteht darin, personalisierte Erfahrungen zu schaffen. Durch die Analyse des Nutzerverhaltens und der Nutzerpräferenzen können Online-Plattformen personalisierte Inhalte, Produktvorschläge und Werbeaktionen anbieten. Diese Personalisierung trägt dazu bei, dass Nutzer relevante Informationen erhalten, die ihren Interessen besser entsprechen.

Web-Tracking ermöglicht die zielgerichtete Auslieferung von Werbung, was einen weiteren Vorteil für die Nutzer darstellt. Durch die Analyse des Nutzerverhaltens können die Plattformen die Werbung gezielt auf die individuellen Interessen und Vorlieben der

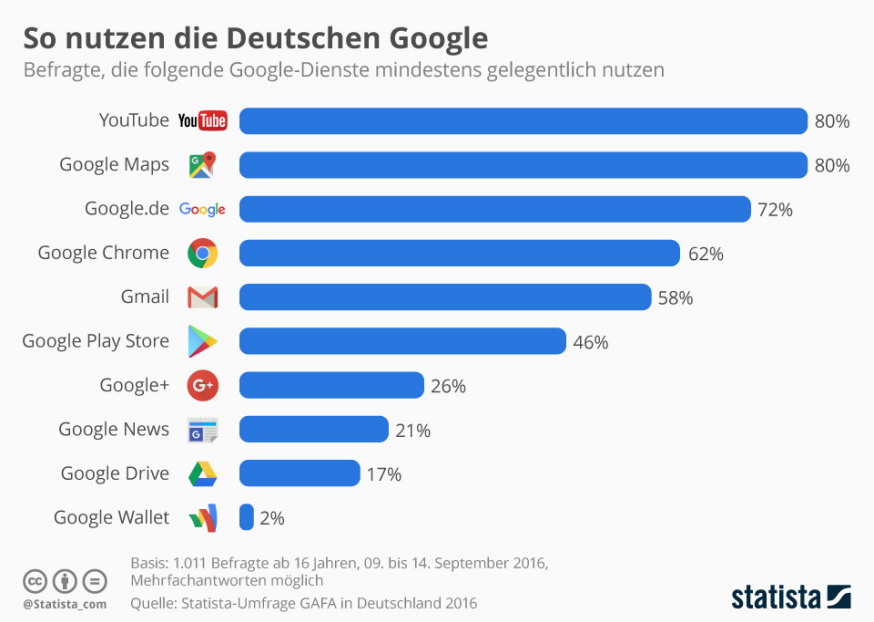


Abbildung 4: Befragung: Wie die Deutschen Google-Dienste nutzen [Bra16]

Nutzer ausrichten. Das bedeutet, dass die Nutzer eher auf für sie relevante Werbung stoßen, anstatt mit irrelevanten Werbebotschaften konfrontiert zu werden.

Ein weiterer wichtiger Aspekt des Web-Trackings ist die Verbesserung des Checkout-Prozesses. Durch die Analyse des Nutzerverhaltens können Online-Plattformen den Kaufprozess effizienter gestalten. Dies trägt nicht nur zur Verbesserung der Konversionsraten bei, sondern ermöglicht auch eine nahtlosere Interaktion zwischen Nutzer und E-Commerce-Plattformen.

4.2 Nutzung kostenloser State-of-the-Art Produkte

Die Nutzung kostenloser, moderner Produkte wie der Google-Suchmaschine, YouTube und Gmail bietet Nutzern zweifellos den Vorteil des kostenfreien Zugangs zu hochwertigen Diensten mit herausragender Leistung, Benutzerfreundlichkeit, umfangreichen Funktionen und nahtloser Integration. Diese Dienste sind für viele Menschen zu integralen Bestandteilen ihres digitalen Alltags geworden, wie die statistische Auswertung der deutschen Google-Befragten zeigt. Trotz der offensichtlichen Vorteile dieser Dienste gibt es jedoch einige wichtige Überlegungen.

Die Nutzung dieser Dienste geht mit berechtigten Datenschutzbedenken einher. Die Plattformen sammeln und analysieren umfangreich Daten, was Bedenken hinsichtlich der Privatsphäre und Datensicherheit aufwerfen kann. Nutzer sollten sich bewusst sein, wie ihre Daten verwendet werden und inwieweit ihre Privatsphäre geschützt ist.

Kostenlose Dienste finanzieren sich oft durch Werbeeinnahmen. Nutzer müssen daher mögliche Störungen durch Werbung in Kauf nehmen. Diese kann nicht nur als lästig empfunden werden, sondern birgt auch die Gefahr von Tracking-Mechanismen, die das Nutzerverhalten verfolgen, um personalisierte Werbung auszuliefern.

Die hohe Nutzungsrate lässt darauf schließen, dass Nutzer stark von diesen Diensten abhängig sind. Dies könnte zu einer gewissen Verwundbarkeit führen, wenn Nutzer plötzlich auf diese Dienste verzichten müssen oder es zu unerwarteten Änderungen in den Nutzungsbedingungen kommt.

Die Nutzer haben oft nur begrenzte Kontrolle darüber, wie ihre persönlichen Daten von diesen Diensten verwendet werden. Um den Nutzern mehr Kontrolle und Verständnis zu ermöglichen, sollte die Transparenz hinsichtlich der Datennutzung und -speicherung verbessert werden.

4.3 Nutzerdatensicherheit: Präventive Maßnahmen

Nutzer können verschiedene Maßnahmen ergreifen, um sich vor Tracking und ungewolltem Sammeln persönlicher Daten zu schützen. Um Internetnutzer und Kunden wiederzuerkennen und Kampagnen- und Analyse-Daten einzelnen Nutzern zuordnen zu können, werden verschiedene Technologien eingesetzt. Dazu gehören unter anderem Cookies, die im Browser-Cache des Nutzers gespeichert werden und eine Cookie-ID, eine Laufzeit und weitere Daten enthalten. Wenn ein Nutzer dieselbe Website oder ein Banner desselben Lösungsanbieters besucht, wird der Browserspeicher von der entsprechenden Marketinglösung ausgelesen. Bekannte Cookies werden wiedererkannt und dem Nutzer auf dem Anbieterserver zugeordnet. So kann beispielsweise eine Customer Journey erstellt werden, die Daten darüber enthält, welche Inhalte und Produkte ein Nutzer angesehen, angeklickt oder gekauft hat. Es ist wichtig, bewusst mit Cookies umzugehen. Regelmäßiges Löschen von Cookies, gezieltes Vorgehen gegenüber Cookie-Bannern und die Präferenz von Session-Cookies tragen zur Datensicherheit bei.

Darüber hinaus können Anti-Tracking-Tools effektive Maßnahmen bieten, um das Tracking persönlicher Daten im Internet zu begrenzen. Es ist empfehlenswert, auf Adblocker zu verzichten und stattdessen den anonymen Modus zu nutzen sowie die Aktivierung von 'Do Not Track' (DNT) in den Browser-Einstellungen vorzunehmen, um die Datensicherheit zu erhöhen. DNT ermöglicht es Nutzern, selbst zu entscheiden, ob sie von Tracking-Software erfasst werden möchten. Allerdings ist seine Effektivität begrenzt, da es keine gesetzlichen Vorgaben für seine Nutzung gibt.

Die Nutzung von Adblockern in Deutschland gibt Einblicke in das Nutzerverhalten. Die Deaktivierungsbereitschaft variiert je nach Inhaltstyp. Online-Shops und journalistische Inhalte stehen mit 22 % an erster Stelle. Überraschenderweise würden 35 % der Nutzer ihren Adblocker für keinen der genannten Inhalte deaktivieren. Gleichzeitig nutzen 41 % Adblocker oder Anti-Tracking-Software. Die Ergebnisse legen nahe, dass die Akzeptanz von Werbung stark von den Inhalten abhängt. Viele Nutzer bevorzugen werbefreie Erfahrungen.

Zusätzlich kann das Deaktivieren des automatischen Ladens von Bildern in E-Mails die Anonymität im Web erhöhen. Dadurch wird verhindert, dass E-Mail-Marketing-Tools Pixel verwenden, um das Öffnen von E-Mails zu verfolgen. Diese praxisorientierten Maßnahmen unterstützen die Nutzer dabei, ihre Online-Privatsphäre zu schützen und informieren darüber, wie sie proaktiv gegen Tracking vorgehen können.

5 Ethische Aspekte des Trackings

Dieses Kapitel behandelt die ethischen Aspekte des Web-Trackings im E-Commerce. Der Fokus liegt auf dem Gleichgewicht zwischen Unternehmensinteressen und Datenschutzrechten. Es wird betont, wie wichtig Transparenz und verantwortungsvoller Umgang mit Nutzerdaten sind, um Vertrauen zu sichern und ethische Standards im digitalen Raum zu fördern.

5.1 Datenschutz: DSGVO

DSGVO ist eine einheitliche Regelung der Europäischen Union zur Verarbeitung personenbezogener Daten durch Unternehmen und Institutionen. Sie gilt EU-weit und hat im Jahr 2018 die vorherige Richtlinie 94/46/EG von 1995 ersetzt. Im Unterschied zu dieser Richtlinie bedarf die DSGVO keiner nationalen Umsetzung durch die Mitgliedsstaaten, sondern entfaltet unmittelbare Wirkung in der gesamten EU. Dieser rechtliche Rahmen etabliert ein einheitliches Datenschutzniveau und stärkt somit den Schutz natürlicher Personen im Zusammenhang mit der Verarbeitung ihrer persönlichen Daten.

5.1.1 Personenbezogene Daten

Gemäß Artikel 4 der DSGVO umfassen personenbezogene Daten sämtliche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Identifizierbarkeit kann direkt oder indirekt erfolgen, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung oder besonderen Merkmalen. Diese Merkmale können die physische,

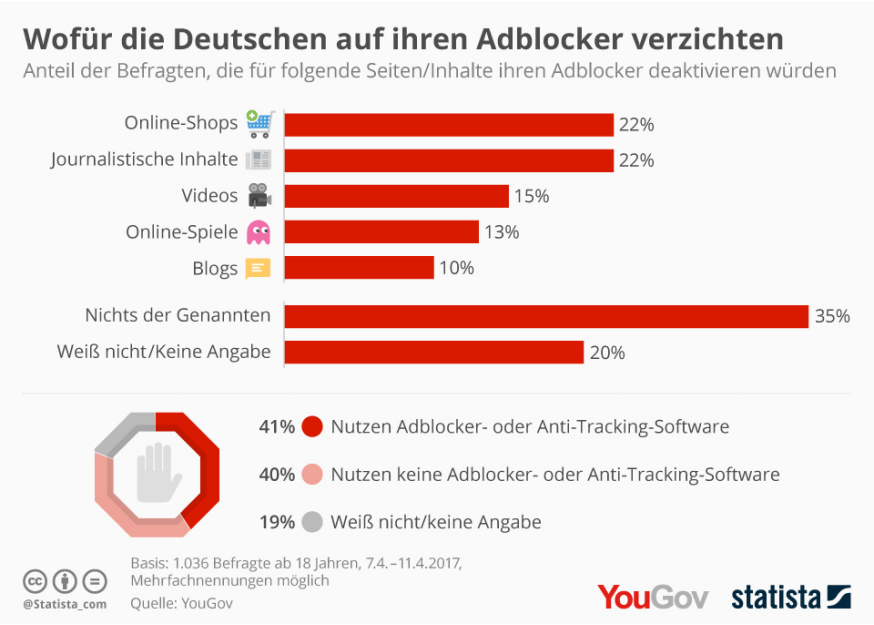


Abbildung 5: Befragung: Wofür die Deutschen auf Ihren Adblocker verzichten [Nie17]

physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität einer Person widerspiegeln. Die präzise Definition unterstreicht den breiten Umfang personenbezogener Daten und bildet die Grundlage für den Schutz der Privatsphäre und den verantwortungsvollen Umgang mit diesen Daten im Rahmen der DSGVO.

Gemäß Artikel 5 der DSGVO sind die Anforderungen an die Verarbeitung personenbezogener Daten in sechs Grundsätzen formuliert. Der erste Grundsatz betont die Notwendigkeit einer nachvollziehbaren Datenverarbeitung und umfasst die Prinzipien von Rechtmäßigkeit, Verarbeitung nach Treu und Glauben sowie Transparenz. Einzelpersonen haben gemäß Artikel 15 das Recht, Informationen über ihre gespeicherten Daten zu erhalten. Zweitens legt der Grundsatz der Zweckbindung fest, dass personenbezogene Daten nur für vorab festgelegte, eindeutige und legitime Zwecke verarbeitet werden dürfen. Drittens erfordert die Datenminimierung, dass die Erhebung und Verarbeitung auf das notwendige Maß beschränkt sind. Der Grundsatz der Richtigkeit verlangt die unverzügliche Korrektur sachlich unrichtiger personenbezogener Daten. Viertens besagt die Speicherbegrenzung, dass Daten nicht länger gespeichert werden dürfen als für den Verarbeitungszweck erforderlich. Das 'Recht auf Vergessenwerden' gemäß Artikel 17 ermöglicht es Personen, die Löschung ihrer Daten zu fordern. Fünftens fordert der Grundsatz der Integrität und Vertraulichkeit angemessene Sicherheitsmaßnahmen zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Verlust, Zerstörung oder Schädigung der Daten. Diese Grundsätze bilden das Grundgerüst der DSGVO und gewährleisten einen ethisch fundierten und transparenten Umgang mit personenbezogenen Daten im E-Commerce.

5.1.2 Einwilligung und Datenschutzerklärung

Gemäß Artikel 83 Absatz 5 der DSGVO ist das datenverarbeitende Unternehmen verpflichtet, die Einhaltung der Datenschutzgrundsätze nachzuweisen. Bei Nichteinhaltung dieser Grundsätze drohen erhebliche Bußgelder und Sanktionen. Artikel 6 betont, dass die Verarbeitung personenbezogener Daten an die eindeutige Einwilligung der betroffenen Person gebunden ist. Die DSGVO empfiehlt die Schriftform für die Einholung der Einwilligung, obwohl dies nicht zwingend vorgeschrieben ist. Außerdem erhöht die DSGVO mit den Artikeln 13 und 14 die rechtlichen Anforderungen an Datenschutzerklärungen. Diese müssen von Onlinehändlern präzise, transparent, verständlich und leicht auffindbar auf der Website abrufbar sein. Die Datenschutzerklärung muss Informationen über Art, Umfang und Zwecke der Datenerhebung und -verwendung enthalten. Außerdem müssen Belehrungen über Widerspruchs- und Widerrufsmöglichkeiten gegeben werden. Eine Integration der Datenschutzerklärung in die Allgemeinen Geschäftsbedingungen (AGBs) ist unzulässig. Der Käufer muss die Kenntnisnahme der Datenschutzerklärung sowie der AGBs bestätigen, um einen Bestellvorgang abzuschließen. Gemäß den DSGVO-Regelungen erfordert der Einsatz von Cookies die Zustimmung des Onlinenutzers. Diese Bestimmungen gewährleisten einen rechtskonformen und transparenten Umgang mit personenbezogenen Daten im E-Commerce.

5.2 Ethische Aspekte

Die ethischen Überlegungen konzentrieren sich darauf, das berechtigte Interesse von Unternehmen an der Datenerhebung für personalisierte Dienste mit den individuellen Datenschutzrechten der Nutzer in Einklang zu bringen. Im E-Commerce-Bereich ist eine transparente Kommunikation über Tracking-Praktiken entscheidend, um das Vertrauen der Verbraucher zu wahren. Ethik im Web-Tracking erfordert den respektvollen Umgang mit persönlichen Daten, die Minimierung von Datensammlung und -speicherung auf das notwendige Maß sowie die klare Zustimmung der Nutzer. Eine kritische Reflexion über die Auswirkungen von Web-Tracking auf die Privatsphäre und Autonomie der Nutzer ist notwendig, um einen ausgewogenen Ansatz zwischen individuellen Rechten und unternehmerischen Interessen zu gewährleisten. Ethik im Web-Tracking sollte nicht nur den gesetzlichen Anforderungen genügen, sondern auch höheren moralischen Standards entsprechen, um eine verantwortungsbewusste und nachhaltige digitale Umgebung zu schaffen.

6 Fazit

Die vorliegende Seminararbeit hat sich intensiv mit dem Thema Online-Tracking und Datenschutz auseinandergesetzt. Die zentrale Erkenntnis ist, dass das Tracking im digitalen Zeitalter sowohl unvermeidlich als auch komplex sind. Profitorientierte Unternehmen, insbesondere in der E-Commerce-Branche, nutzen verschiedene Technologien wie Cookies, Tracking-Pixel und Event Tracking, um Nutzerdaten zu sammeln und zu analysieren. Diese Daten werden zur Personalisierung und Optimierung des Nutzererlebnisses verwendet, was sowohl Vorteile als auch Nachteile mit sich bringt.

Auf der einen Seite bietet das Tracking den Nutzern erhebliche Vorteile, wie z.B. den Zugang zu kostenlosen und hochmodernen Produkten und Dienstleistungen. Andererseits wirft es Bedenken hinsichtlich der Privatsphäre und der Sicherheit der Nutzerdaten auf. Die ethischen Aspekte des Trackings, insbesondere im Hinblick auf die Einhaltung der DSGVO, die Verarbeitung personenbezogener Daten und die Notwendigkeit der Einwilligung, sind komplex und erfordern eine ständige Überwachung und Anpassung.

Aus unserer persönlichen Sicht erscheint das Modell, bei dem mit Daten die kostenfreie Nutzung einer hochmodernen Software bezahlt wird, alternativlos. Bei einer eigenen Analyse von Konkurrenzprodukten wie DuckDuckGo die keine Daten sammeln, fällt auf, dass deren Suchergebnisse deutlich weniger umfangreich sind als die der Google-Suchmaschine. [Wei23] Dies unterstreicht die Effizienz und Qualität datenbasierter Dienste. Eine Alternative könnte ein Abo-Modell sein, bei dem die Nutzer eine monatliche Gebühr für die Nutzung von Diensten wie der Google-Suchmaschine zahlen. In diesem Szenario würde kein Tracking stattfinden, was den Schutz der Privatsphäre, den Verzicht auf personalisierte Werbung und die Reduzierung von Impulskäufen bedeuten würde.

Für viele Nutzer stellt sich diese Option jedoch als „Alles oder Nichts“-Szenario dar. Es muss eine Balance zwischen dem Wunsch nach Datenschutz und dem Bedürfnis

nach qualitativ hochwertigen, personalisierten Online-Diensten gefunden werden. Eine mögliche, wenn auch unwahrscheinliche Lösung könnte die Einführung von Richtlinien durch staatliche Stellen oder die EU sein, die die Datensammlung durch Big-Tech-Unternehmen einschränken und gleichzeitig den Nutzern qualitativ hochwertige Dienste bieten.

Zusammenfassend lässt sich sagen, dass die Diskussion um Online-Tracking und Datenschutz ein wichtiges Thema bleiben wird, das sowohl von Unternehmen als auch von Regulierungsbehörden ständige Aufmerksamkeit und Anpassungen erfordert. Die Herausforderung besteht darin, eine Balance zwischen Nützlichkeit und Privatsphäre zu finden, die sowohl den Bedürfnissen der Nutzer als auch den Interessen der Unternehmen gerecht wird. Die Zukunft wird zeigen, ob und wie neue Modelle und Richtlinien entwickelt werden können, um eine faire und transparente Datenlandschaft zu schaffen.

Abschließend bleibt festzuhalten, dass die Diskussion um Datenschutz und Online-Tracking ein dynamisches Feld ist, das einer ständigen Beobachtung und Anpassung bedarf. Während das derzeitige Modell des Datenaustauschs für kostenlose Dienste weit verbreitet ist, eröffnen sich mit der Zeit neue Möglichkeiten und Herausforderungen. Ein Abonnementmodell könnte eine interessante Alternative darstellen, erfordert jedoch sorgfältige Überlegungen und möglicherweise einen kulturellen Wandel in der Wahrnehmung von Online-Diensten. Ebenso könnte die Rolle staatlicher und supranationaler Regulierungsbehörden an Bedeutung gewinnen, um ein faireres und sichereres digitales Umfeld zu schaffen. Letztendlich wird die Entwicklung in diesem Bereich sowohl von technologischen Innovationen als auch von gesellschaftlichen und rechtlichen Veränderungen abhängen.

7 Ausblick

Die digitale Zukunft wird wesentlich durch die Monopolstellung der *Big Five* Technologieunternehmen und die wachsenden Herausforderungen für den Datenschutz, insbesondere im Zusammenhang mit Google Analytics, geprägt sein.

Die Dominanz von Google, Amazon, Facebook, Apple und Microsoft, verstärkt durch ihre umfangreichen Datensammlungen, bleibt eine zentrale Herausforderung für Wettbewerb und Datenschutz. Dies könnte zu verstärkten regulatorischen Eingriffen führen, um faire Marktbedingungen und den Schutz der Nutzerdaten zu gewährleisten.

Gleichzeitig steht der Einsatz von Google Analytics in der EU zunehmend unter rechtlicher Beobachtung, insbesondere nach den Klagen von Max Schrems und noyb. Die ersten Urteile gegen Google Analytics verdeutlichen den wachsenden Druck auf EU-Unternehmen, datenschutzfreundliche Alternativen zu nutzen. Dies könnte eine Wende hin zu strengeren Datenschutzbestimmungen und einer Einschränkung des Datentransfers in Drittstaaten bedeuten. [Eve23]

Insgesamt sind signifikante Veränderungen in Bezug auf Datenschutz, Datensicherheit und Marktdynamik zu erwarten, die neue Herausforderungen und Chancen für Unternehmen und Nutzer mit sich bringen.

Literaturverzeichnis

[Ana23] Stock Analysis. *Amazon Revenue 2023*. Abgerufen am: 14.01.2024. 2023. URL: https://stockanalysis.com/stocks/amzn/revenue/.

[Arp+16] Daniel Arp u. a. *Bat in the Mobile: A Study on Ultrasonic Device Tracking*. Computer Science Report 2016-02. Institute of System Security: Technische Universität Braunschweig, 2016.

[Axc23] Axciom. *Datennutzung in deutschen Unternehmen in der Post-ThirdParty-Cookie-Ära*. Abgerufen am: 14.01.2024. 2023. URL: https://www.acxiom.de/wp-content/uploads/2023/10/acxiom_datenschutz_studie_2023_web_version.pdf.

[Ber18] C. Berg. Web Tracking im E-Commerce. *Online-Medien-Management, Band 7*. Hrsg. von B. Schwarzer und S. Spitzer. Nomos Verlagsgesellschaft/Edition Reinhard Fischer, 2018, S. 63–64. URL: https://www.nomos-shop.de/en/nomos/title/web-tracking-im-e-commerce-id-68704/.

[Boc23] René Bocksch. *Vom Handy ausspioniert?* Abgerufen am: 14.01.2024. 2023. URL: https://de.statista.com/infografik/29641/anteil-der-befragten-die-werbung-zu-kuerzlich-erwaehnten-produkten-wahrnehmen.

[Bra16] Mathias Brandt. *So nutzen die Deutschen Google*. Abgerufen am: 14.01.2024. 2016. URL: https://de.statista.com/infografik/6020/nutzung-von-google-diensten-in-deutschland/.

[Eve23] Dr. Evelyne Sørensen. *Das Ende von Google Analytics in Europa?* Abgerufen am: 14.01.2024. 2023. URL: https://www.activemind.de/magazin/google-analytics-datenschutz/.

[Fit20] Aidan Fitzpatrick. *Who's watching who? Netflix and your data*. Abgerufen am: 14.01.2024. 2020. URL: https://reincubate.com/blog/netflix-data-tracking/.

[Gar+18] Jean Garcia-Gathright u. a. *Understanding and Evaluating User Satisfaction with Music Discovery*. Abgerufen am: 14.01.2024. 2018. URL: https://research.atspotify.com/2018/07/understanding-and-evaluating-user-satisfaction-with-music-discovery.

[Ion22] Ionos. *Tracking Pixel – so einfach funktioniert modernes Tracking*. Abgerufen am: 14.01.2024. 2022. URL: https://www.ionos.de/digitalguide/online-marketing/web-analyse/was-ist-ein-tracking-pixel.

[Kan21] Tanya Kant. *A History of the Data-Tracked User*. Abgerufen am: 14.01.2024. 2021. URL: https://thereader.mitpress.mit.edu/a-history-of-the-data-tracked-user.

[Kol19] Tobias Kollmann. *E-Business. Grundlagen elektronischer Geschäftsprozesse in der Digitalen Wirtschaft*. Springer Gabler, 2019, S. 431–432. URL: https://doi.org/10.1007/978-3-658-26143-6.

[MSO] MSO-Digital. *Event Tracking*. Abgerufen am: 14.01.2024. URL: https://www.mso-digital.de/wiki/event-tracking.

[Nie17] Hedda Nier. *Wofür die Deutschen auf ihren Adblocker verzichten*. Abgerufen am: 14.01.2024. 2017. URL: https://de.statista.com/infografik/9025/wofuer-die-deutschen-auf-ihren-adblocker-verzichten/.

[Phi23] Matt Philipps. *The SP 500's gains are almost entirely from just five companies*. Abgerufen am: 14.01.2024. 2023. URL: https://www.axios.com/2023/06/01/sp500-tech-companies-stock-price.

[Pro11] Emil Protalinski. *Facebook denies cookie tracking allegations*. Abgerufen am: 14.01.2024. 2011. URL: https://www.zdnet.com/article/facebook-denies-cookie-tracking-allegations/.

[Ryt] Ryte. *Event Tracking*. Abgerufen am: 14.01.2024. URL: https://de.ryte.com/wiki/Event_Tracking.

[Sta23a] Statcounter. *Search Engine Market Share Worldwide*. Abgerufen am: 14.01.2024. 2023. URL: https://gs.statcounter.com/search-engine-market-share.

[Sta23b] Statista. *Die größten Technologieunternehmen der Welt nach Umsatz und Marktwert im Jahr 2023*. Abgerufen am: 14.01.2024. 2023. URL: https://de.statista.com/statistik/daten/studie/1309854/umfrage/top-technologieunternehmen-der-welt-nach-marktwert-und-umsatz.

[Ung23] Lisa-Marie Unger. *Event Tracking: Interaktionen auf der Website messen und Usability optimieren*. Abgerufen am: 14.01.2024. 2023. URL: https://www.netpulse.ch/wissen/event-tracking.

[Wei23] Gabriel Weinberg. *Is DuckDuckGo a Good Search Engine?* Abgerufen am: 14.01.2024. 2023. URL: https://spreadprivacy.com/is-duckduckgo-a-good-search-engine/.

[Wik23a] Wikipedia. *Cross-Device-Tracking*. Abgerufen am: 14.01.2024. 2023. URL: https://de.wikipedia.org/wiki/Cross-Device_Tracking.

[Wik23b] Wikipedia. *Zählpixel*. Abgerufen am: 14.01.2024. 2023. URL: https://de.wikipedia.org/wiki/Z%C3%A4hlpixel.

Anlage

Auf den folgenden Seiten finden Sie eine gedruckte, kompaktere und anschaulichere Version dieser Seminararbeit. Diese Version wurde als interaktives Plakat unter Verwendung von WordPress gestaltet. Bitte beachten Sie, dass einige interaktive Elemente in der gedruckten Fassung möglicherweise nicht korrekt wiedergegeben werden, da diese normalerweise dynamisch geladen werden, sobald ein Nutzer die Webseite aufruft. Für die Druckversion wurden die Seiteninhalte daher als statisches PDF festgehalten.

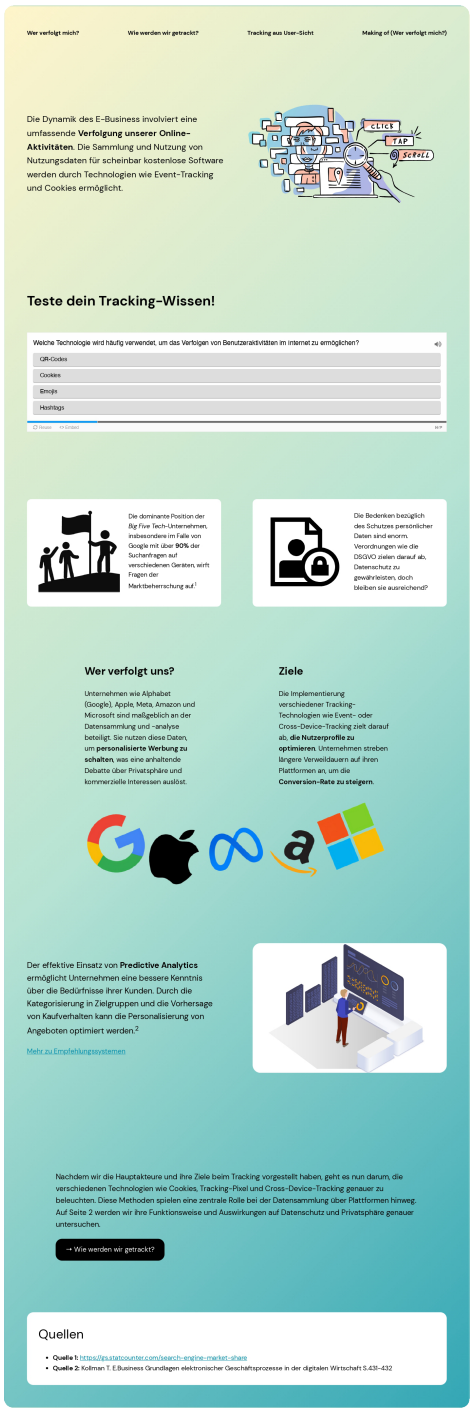


Abbildung 6: Wer verfolgt mich? - Die Krux mit dem Tracking (CX)

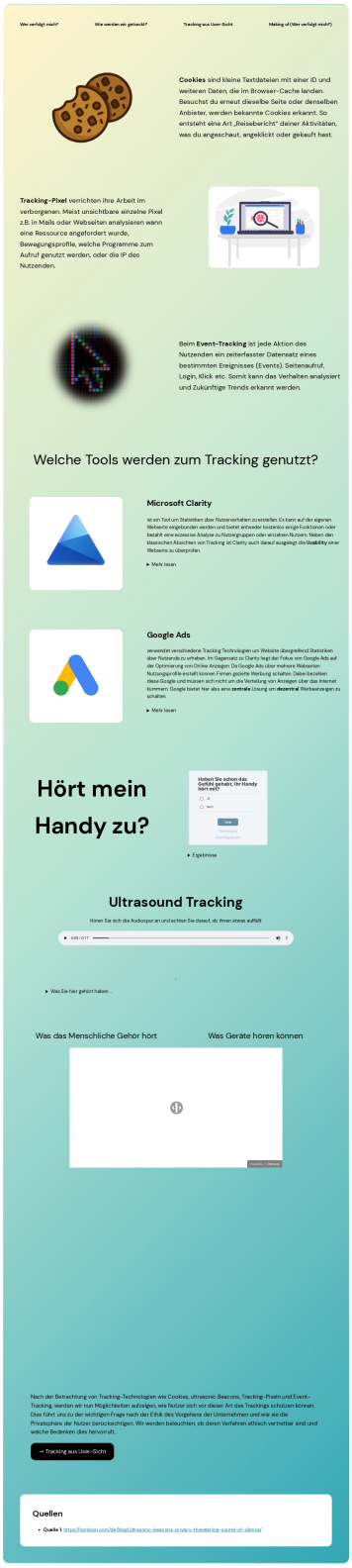


Abbildung 7: Wir werden wir getrackt?

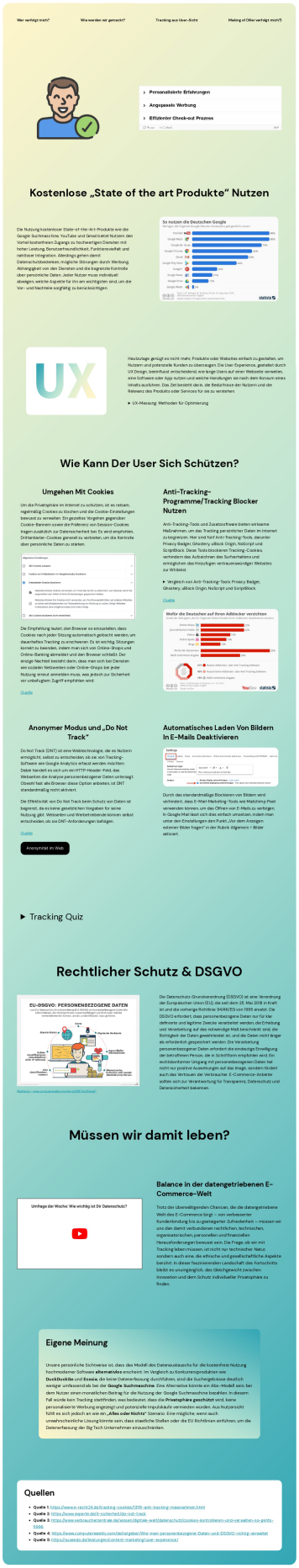


Abbildung 8: Tracking aus User-Sicht

Abbildung 9: Making Of (Wer verfolgt mich?)

Hochschule Düsseldorf
University of Applied Sciences

Fachbereich Medien
Faculty of Media

Datenbanken und E-Business
Databases and E-Business

Wie gut, dass keiner weiß – Anonymität im Web (inklusive Dark Net)

Seminararbeit „Problemfälle des E-Business“

Till Büge
Sven Schoop
Luca Selinski

März 2024

Modul E-Business
WS 2023/2024

Master Medieninformatik

Fachbereich Medien
Hochschule Düsseldorf

Inhaltsverzeichnis

Kurzfassung

In dieser Arbeit wird ein umfassender Überblick über die Entwicklung und die gegenwärtige Bedeutung von Anonymität im Internet, einschließlich des Dark Nets, gegeben. Durch die Analyse verschiedener wissenschaftlicher Arbeiten beleuchten wir die vielschichtigen Aspekte und Auswirkungen der Anonymität im Web. Wir diskutieren technische Mittel zur Wahrung der Anonymität, wie den Tor-Browser und VPNs, und betrachten die sozialen Implikationen von Anonymität auf individueller, gruppenspezifischer und politischer Ebene. Besonderes Augenmerk liegt auf den positiven und negativen Folgen von Anonymität, insbesondere in Bezug auf Datenschutz, Meinungsfreiheit und Cyberkriminalität. Unsere Analyse verdeutlicht, dass Anonymität im Internet ein komplexes Phänomen ist, das je nach Nutzung positive und negative Effekte haben kann. Diese Arbeit schließt mit einem Ausblick auf zukünftige Forschungsrichtungen ab, unterstreicht die Notwendigkeit einer ausgewogenen Betrachtung und diskutiert die Herausforderungen bei der Bekämpfung von Cyberkriminalität im Dark Web, während gleichzeitig die Privatsphäre und Sicherheit der Nutzer geschützt werden.

This work provides a comprehensive overview of the development and current significance of anonymity on the Internet, including the dark net. By analysing various scientific papers, we shed light on the complex aspects and effects of anonymity on the web. We discuss technical means of maintaining anonymity, such as the Tor browser and VPNs, and consider the social implications of anonymity on an individual, group and political level. Particular attention is paid to the positive and negative consequences of anonymity, especially in relation to data protection, freedom of expression and cybercrime. Our analysis makes it clear that anonymity on the Internet is a complex phenomenon that can have positive and negative effects depending on how it is used. This paper concludes with an outlook on future research directions, emphasises the need for a balanced view and discusses the challenges of combating cybercrime on the dark web while protecting user privacy and security.

Anonymität, Internet, Dark Web, Cyberkriminalität

5533 Wörter

1 Einleitung

Das Web, einst eine Innovation, die die Art und Weise, wie wir kommunizieren, Informationen austauschen und Geschäfte betreiben, revolutioniert hat, ist heute ein integraler Bestandteil des täglichen Lebens. Mit dieser Entwicklung ist das Bedürfnis nach Anonymität im Web gewachsen, ein Thema, das sowohl faszinierend als auch kontrovers ist. Viele Menschen suchen Anonymität im Web – diese hat jedoch sowohl positive als auch negative Implikationen und ist daher Gegenstand vieler Diskussionen und wissenschaftlicher Untersuchungen.

Die historische Entwicklung der Anonymität im Web ist eng verknüpft mit dem Wachstum des Internets selbst. Anfangs als ein Mittel für freie und offene Kommunikation gefeiert, wurde das Web schnell zu einem Raum, in dem Datenschutz und Anonymität zu kritischen Themen wurden. Die Einführung des Dark Webs hat diese Diskussionen noch intensiviert, da es sowohl für legitime Zwecke der Privatsphäre als auch für kriminelle Aktivitäten genutzt wird.

Ein aktuelles Beispiel, das die Bedeutung von Anonymität im Web unterstreicht, ist eine Umfrage unter Online-Nutzern in den Vereinigten Staaten aus dem dritten Quartal 2022 [1], welche in Abbildung 1 dargestellt ist. Laut dieser Studie lehnen 43,2% der Internetnutzer zumindest gelegentlich Cookies auf Websites ab. Dies deutet darauf hin, dass ein signifikanter Teil der Internetnutzer besorgt um ihre Online-Privatsphäre ist und aktive Schritte unternimmt, um diese zu schützen. Noch aussagekräftiger ist, dass 41,2% der Befragten sich Sorgen darüber machen, wie Unternehmen ihre Online-Daten verwenden könnten, was die Bedenken hinsichtlich der Datennutzung und -sicherheit im digitalen Raum widerspiegelt. Besonders relevant für diese Arbeit ist, dass 33,6% der Nutzer es vorziehen, beim Einsatz von Online-Diensten anonym zu bleiben. Diese Zahl veranschaulicht das wachsende Bedürfnis nach Anonymität im digitalen Zeitalter und dient als Grundlage für die

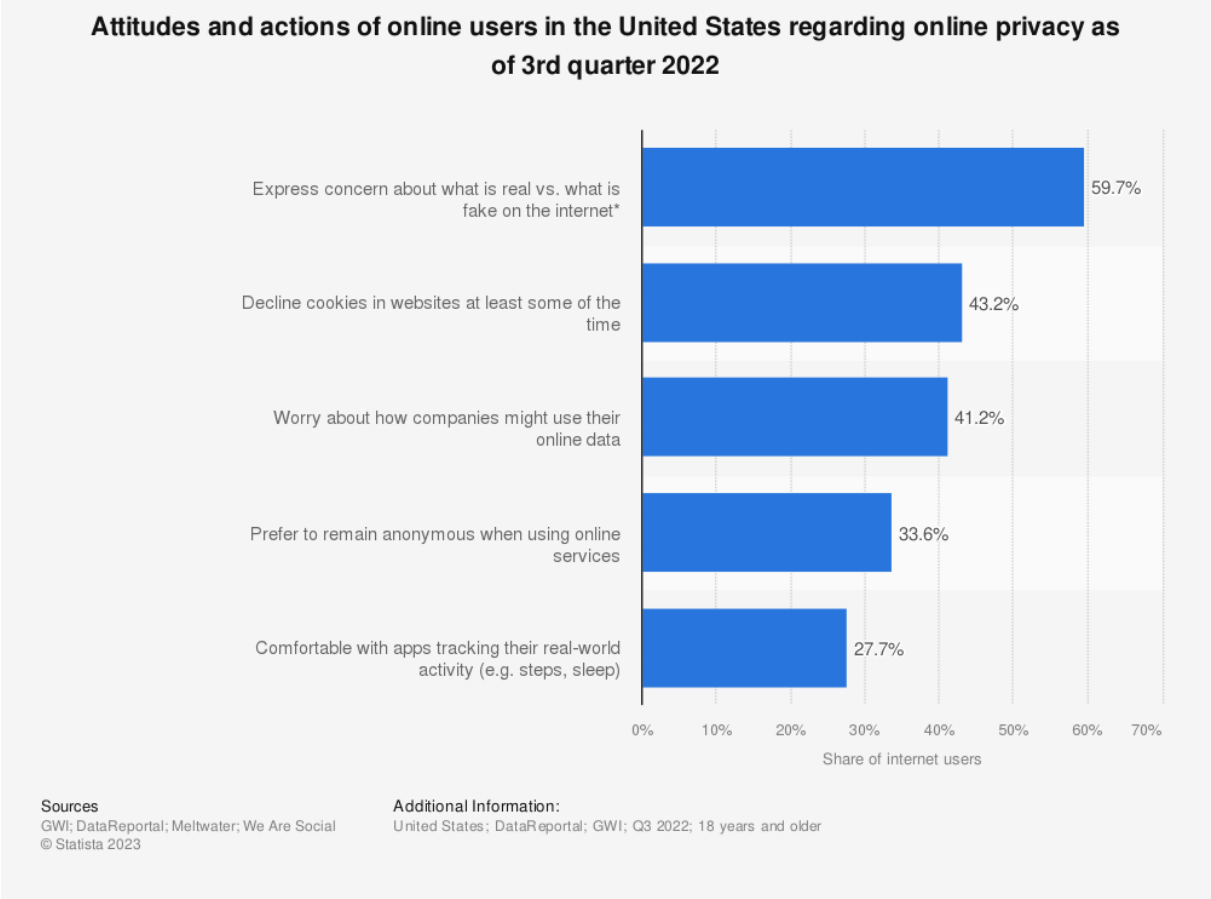


Abbildung 1: Haltungen und Handlungen von Online-Nutzern in den Vereinigten Staaten bezüglich des Online-Datenschutzes im 3. Quartal 2022

tiefgehende Betrachtung der Auswirkungen und Mechanismen der Anonymität im Web, die in dieser Arbeit untersucht werden [1].

Angesichts der wachsenden Bedeutung und Komplexität der Anonymität im Web stellt sich unsere Arbeit der Herausforderung, diese tiefgehend zu untersuchen. Die zentrale Forschungsfrage lautet:

Wie beeinflussen Definition und Praxis von Anonymität im Web, einschließlich des Dark Webs, soziale Interaktionen und ethische Normen, und wie können die daraus resultierenden Vorteile und Risiken ausbalanciert werden?

Diese Frage zielt darauf ab, die vielschichtigen Dimensionen der Anonymität zu erforschen, von den technischen Mechanismen, die sie ermöglichen, bis hin zu ihren sozialen und ethischen Auswirkungen. Durch die Beantwortung dieser Frage beabsichtigen wir, ein umfassendes Verständnis der Rolle von Anonymität im digitalen Zeitalter zu entwickeln und gleichzeitig die Balance zwischen Privatsphäre und Transparenz, Freiheit und Sicherheit zu erörtern.

Diese Arbeit gliedert sich in mehrere Schlüsselbereiche, um die vielfältigen Aspekte der Anonymität im Web umfassend zu beleuchten. Nach der Einleitung beginnen wir mit einer detaillierten Betrachtung der verschiedenen Definitionen von Anonymität und den technischen Mitteln ihrer Implementierung. Es folgt eine Analyse der sozialen Auswirkungen von Anonymität, sowohl auf individueller als auch auf Gruppenebene, und eine Diskussion über deren Einfluss auf Menschenrechte und die zugrunde liegenden Theorien. Ein besonderes Augenmerk wird auf das Dark Web gelegt, um dessen Funktionsweise und die daraus resultierenden Auswirkungen zu verstehen. Das Fazit fasst die Schlüsselerkenntnisse zusammen und reflektiert über Anonymität im Kontext der technischen Identifikation und sozialen Aspekte. Der abschließende Ausblick gibt einen Überblick über mögliche zukünftige Entwicklungen in diesem Bereich.

2 Beschreibung der Ergebnisse

In diesem Kapitel wird die zugrundeliegende Recherche vorgestellt, die gefundenen wissenschaftlichen Artikel kurz zusammengefasst und die Inhalte der Artikel nach Thema eingeordnet, kategorisiert und verglichen.

2.1 Recherche

Für die Zusammenstellung der Quellen unserer Seminararbeit haben wir zunächst durch die Verwendung passender Stichworte über Google Scholar und die Suche der Hochschul-Bibliothek eine breite Auswahl an wissenschaftlichen Arbeiten identifiziert, die unserer Forschungsfrage entsprechen. Dieser erste Schritt ermöglichte es uns, eine umfassende Perspektive auf bestehende Literatur zu gewinnen.

Hierbei lag der Fokus auf einer gezielten Auswahl von Büchern, Fachzeitschriften und Konferenzbeiträgen. Dabei haben wir besonders auf die Anzahl der Zitationen geachtet, um die wissenschaftliche Anerkennung der Quellen zu beurteilen, und das Renommee der Konferenzen berücksichtigt, auf denen die Forschung präsentiert wurde.

Um sicherzustellen, dass unsere Seminararbeit auf etablierter Forschung aufbaut, haben wir schließlich auch in den verschiedenen Quellen zitierte Artikel einbezogen. Diese Herangehensweise ermöglicht es uns, auf bereits anerkannte Arbeiten zurückzugreifen und gleichzeitig die Verlässlichkeit und Glaubwürdigkeit unserer eigenen Recherche zu stärken.

Christopherson [2] erforscht die immer größer werdende Bedeutung der Anonymität in der computervermittelten Kommunikation (CMC) im Kontext des Internetwachstums und bietet einen

Überblick über relevante Literatur sowie die Nützlichkeit sozialpsychologischer Theorien zur Erklärung von Verhalten in CMC und eignet sich dadurch als Einstieg in das Thema der Anonymität im Internet, vor allem auf die sozialen Aspekte bezogen. Der Artikel diskutiert zudem aktuelle theoretische Ansätze zu den Auswirkungen der Anonymität auf soziales Verhalten in CMC und schlägt mögliche Richtungen für zukünftige Forschung vor.

Die Nutzung und Erreichbarkeit von Anonymität im Internet sowie deren Vor- und Nachteile werden in einem Beitrag von Palme und Berglund [3] untersucht. Dabei werden auch die rechtlichen Aspekte, insbesondere die Möglichkeit einer gemeinsamen EU-Richtlinie zur Regulierung der Anonymität in den Mitgliedsstaaten, betrachtet.

Die Forschungsarbeit von Ruogu und Brown [4] wiederum untersucht die Gründe und Methoden, warum Menschen in ihren Online-Interaktionen Anonymität anstreben, mit dem Ziel, relevante Informationen für politische Entscheidungen und die Gestaltung zukünftiger Internetstrukturen und -anwendungen zu liefern. Die Untersuchung basiert auf einer Befragung (n = 44) aus verschiedenen Kontinenten, die Anonymität suchten, und hebt die vielfältigen Erfahrungen und Lebenssituationen der Befragten sowie die Implikationen für Online-Gemeinschaften, politische Herausforderungen und die Verbesserung von Anonymitätstools hervor, wodurch die sozialen Aspekte der Anonymität beleuchtet werden.

Die Publikation von Englehardt et. al. [5] beleuchtet die technische Seite der Anonymität im Internet und untersucht die Fähigkeit eines passiven Abhörers, HTTP-Tracking-Cookies von Drittanbietern für Massenüberwachung zu nutzen, insbesondere wenn zwei Webseiten denselben Tracker verwenden. Die Autoren stellen fest, dass der Angreifer mithilfe dieser Methode 62-73 % des Surfverhaltens eines typischen Benutzers rekonstruieren kann und analysieren die Auswirkungen des physischen Standorts des Abhörgeräts sowie rechtliche Beschränkungen.

Einen Überblick über das Dark Web bietet der Beitrag von Kaur und Randhawa [6]. Es diskutiert Funktionen, verschiedene Browser, Vor- und Nachteile des Dark Webs sowie unterschiedliche Arten von Angriffen und kriminellen Aktivitäten, um Lesern ein Bewusstsein dafür zu vermitteln und mögliche Präventivmaßnahmen zu ermöglichen.

Eine weitere Quelle zum Dark Web ist die Publikation von Jardine [7], die die ambivalente Natur von Online-Anonymitätssystemen wie dem Onion Router (Tor) und dem damit ermöglichten Dark Web diskutiert. Die positiven Aspekte des Dark Webs seien in repressiven Ländern vertreten, wohingegen die negativen Aspekte in liberalen Ländern auftreten. Es wird geschlussfolgert, dass das Dark Web in liberalen Ländern stärker reglementiert werden sollte, um die negativen Auswirkungen zu minimieren und gleichzeitig die positiven Aspekte der Anonymität zu erhalten.

Der Artikel von Chertoff [8] befasst sich ebenfalls mit dem möglichen Umgang einer Regulierung des Dark Webs und den daraus resultierenden Folgen für die Anonymität von Nutzern. Bisherige Erfolge bei der Bekämpfung von Cyberkriminalität werden verglichen und angewandte Taktiken bewertet.

Die Meta-Analyse von Clark-Gordon et. al. [9] beleuchtet wiederum die sozialen Aspekte. Sie untersucht die Beziehung zwischen Anonymität und Online-Selbstoffenbarung als eine Form der gutartigen Enthemmung. Die Ergebnisse zeigen eine durchschnittlich positive Korrelation, obwohl erhebliche Heterogenität zwischen den Studien festgestellt wurde, die nicht durch verschiedene Moderatoren erklärt werden konnte.

Schlussendlich werden die positiven und negativen Aspekte der Anonymität in modernen westlichen Demokratien von Boyd und Field [10] untersucht und vorgestellt. Sie erstellen ein normatives Framework, mit dem Anonymität bewertet werden kann.

2.2 Begriffsdefinitionen

Die verschiedenen wissenschaftlichen Publikationen definieren jeweils unterschiedliche Aspekte der Anonymität:

Laut Christopherson [2] wird Anonymität traditionell als Unfähigkeit anderer, eine Person zu identifizieren oder sich selbst zu identifizieren, definiert. Sie kann in zwei Hauptkategorien unterteilt

werden: Die technische Anonymität und die soziale Anonymität [2, pp. 3039-3040]. Die technische Anonymität enthält die Entfernung aller bedeutenden Identifikationsmerkmale in der Kommunikation. Sie kann z.B. das Entfernen von Namen oder anderen identifizierenden Informationen aus der Internetkommunikation umfassen [2, p. 3040]. Die soziale Anonymität ist dann gegeben, wenn eine Person als unidentifizierbar wahrgenommen wird, wenn es keine Hinweise gibt, dieser Person eine Identität zuordnen zu können. Dies muss aber nicht bedeuten, dass die Person tatsächlich anonym ist, sondern sich nur als anonym wahrnimmt [2, p. 3040].

Zusätzlich kann man zwischen Anonymität und Pseudonymität unterscheiden, wie Palme [3, p. 1] erwähnt. Letzteres liegt vor, wenn ein Nutzer unter einem Pseudonym oder Alias, also einem (selbst-)gewähltem, eventuell erfundenem Namen auftritt, zur Verschleierung der wahren Identität des Nutzers. Durch das Pseudonym können jedoch verschiedene Beiträge eines Nutzers zugeordnet werden, merken Ruogu und Brown [4, p. 2662] an.

Je nach Blickwinkel können verschiedene Vor- und Nachteile einer Anonymität im Internet gefunden werden.

2.3 Technische Identifikation

Die (eindeutige) Identifikation eines Nutzers bzw. die Aufhebung seiner Anonymität kann durch verschiedene Daten und deren Kombination erfolgen, wie Ruogu und Brown [4, p. 2658] beschreiben. Dazu gehören u.a. Name, Aufenthaltsort, Pseudonyme, die Rückschlüsse auf die wahre Identität ermöglichen, Verhaltensmuster, Mitgliedschaft in einer sozialen Gruppe, Informationen bzw. Gegenstände oder Fähigkeiten, die auf die persönliche Charakteristik hinweisen. Außerdem auch technische Daten, wie z.B. die IP-Adresse. Im Folgenden werden überblicksweise zwei verschiedene Arten und Weisen vorgestellt, wie eine technische Identifikation gelingen kann.

Der Einsatz von Third-Party Tracking-Cookies kann sogar zur Massenüberwachung genutzt werden [5, p. 292]. Cookies sind kleine Textdateien, die von Webseiten im Browser gesetzt werden können. Verwenden mehrere Webseiten denselben Tracking-Cookie lassen sich Besuche verschiedenster Webseiten auf den gleichen Nutzer zurückverfolgen, auch wenn sich z.B. die IP-Adresse ändert [5].

ISPs (Internet Service Provider, also Internetanbieter) besitzen viele Möglichkeiten Nutzer eindeutig zu identifizieren. Durch die Bereitstellung der Internetverbindung nehmen die ISPs die Zuordnung der IP-Adressen zu den Kunden, die dem ISP mit Klarnamen und Adresse bekannt sind, vor [3, p. 5]. Außerdem wird der gesamte Netzwerkverkehr zuerst über die Infrastruktur des ISPs geroutet, bevor das eigentliche Internet erreicht wird.

2.4 Soziale Aspekte

Anonymität im Web beeinflusst das menschliche Verhalten auf vielfältige Weise, wie die Arbeiten von Christopherson [2] und Clark-Gordon et al. [9] zeigen. Während Christopherson die Bedeutung der Privatsphäre für das psychische Wohlbefinden betont und auf die potenziellen Gefahren der Anonymität wie die Verstärkung aggressiven Verhaltens oder Isolationsgefühle auf persönlicher, gruppenbasierter und politischer Ebene hinweist [2, pp. 3040-3041], beleuchten Clark-Gordon et al. die komplexen Beziehungen zwischen Anonymität und Selbstoffenbarung in der Online-Kommunikation [9, pp. 99-109].

2.4.1 Persönliche Ebene

Von Christopherson [2] vorgestellte Studien zeigen, dass Privatsphäre wichtig für das psychische Wohlbefinden ist. Ein entscheidender Faktor ist dabei die Kontrolle selbst entscheiden zu können, wann und wie die Privatsphäre aufgeweicht wird (Selbstbestimmung) [2, p. 3040]. Anonymität trägt zur

Erholung, Autonomie und Katharsis, dem Ausdruck von Gedanken und Gefühlen, bei, außerdem kann sie die Selbstakzeptanz und Identität stärken [2, p. 3041].

Andere zitierte Studien zeigen jedoch, dass durch Anonymität aggressives Verhalten, Selbstmordversuche oder andere negative Verhaltensmuster verstärkt werden können. Eine gesteigerte Anonymität kann auch zu einem Isolationsempfinden führen [2, pp. 3040-3041].

2.4.2 Gruppenebene

Ebenso kann eine größere Anonymität in Gruppen zu mehr neuen Argumenten in Diskussionen und einem stärkeren Wettbewerb um kreative Ideen führen, wie Christopherson anmerkt [2, pp. 3042-3044].

In anonymem Gruppen kann es zu einer erhöhten Polarisierung kommen. Außerdem kann die Apathie gesteigert und Hemmungen verringert werden, wodurch es sogar zu gefährlichen Gruppendynamiken kommen kann: Einerseits vermehrt auftretendes antisoziales Verhalten, andererseits eine ausbleibende Intervention durch andere Gruppenmitglieder. Dies wird u.a. in der Deindividuationstheorie beschrieben [2, p. 3044].

2.4.3 Politische Ebene

Anonymität schützt vor Zensur und politischer Verfolgung, genauso wird die Pressefreiheit und Meinungsfreiheit gestärkt. Damit ist Anonymität ein wichtiges Werkzeug Demokratie zu stärken, insbesondere in regimeähnlichen Ländern, und Menschenrechte zu wahren (vgl. [4, p. 2663] oder [7, p. 5]).

Allerdings bietet die Anonymität auch die Möglichkeit durch z.B. die Verbreitung von Falschinformationen oder das Begehen von Straftaten, die durch ebendiese Anonymität nicht verfolgt oder verhindert werden können, die Demokratie zu schwächen [10, p. 339].

2.4.4 Auswirkungen auf die Selbstoffenbarung

Clark-Gordon et al. [9] untersuchen die Beziehung zwischen Anonymität und Selbstoffenbarung, der Preisgabe von persönlichen Informationen an andere, zu denen diese noch keinen Zugang haben oder von denen sie noch nichts wissen, in der Online-Kommunikation. Die Studie unterstreicht die Komplexität der Online-Selbstoffenbarung und stellt fest, dass verschiedene Formen der Anonymität und unterschiedliche Plattformen die Selbstoffenbarung unterschiedlich beeinflussen können [9, pp. 99-100]. Es ist wichtig, Anonymität als ein Kontinuum und nicht als einen binären Zustand zu betrachten, um ihre nuancierten Auswirkungen auf das Online-Verhalten zu verstehen [9, pp. 99-100].

Die Studie kommt zu dem Schluss, dass zwar ein allgemeiner positiver Zusammenhang zwischen Anonymität und Selbstoffenbarung besteht, dass diese Beziehung jedoch sehr heterogen ist, was eine differenziertere Forschung erfordert [9, pp. 107-109]. Die Ergebnisse deuten darauf hin, dass Faktoren wie der Interaktionskontext, die Art der Anonymität und die Art und Weise, wie die Selbstoffenbarung umgesetzt wird, diese Beziehung beeinflussen könnten, obwohl die aktuelle Forschung nicht ausreicht, um diese Faktoren zu bestätigen [9, pp. 107-109].

2.4.5 Theorien zu sozialen Auswirkungen

Die Untersuchung der Anonymität in der computervermittelten Kommunikation (CMC) wurde maßgeblich von vier Theorien beeinflusst: Zimbardos Deindividuationstheorie, die Equalization Hypothesis, das Social Identity Model of Deindividuation Effects (SIDE) und die Adaptive Structuration Theory [2, pp. 3044-3051]. Diese Theorien untersuchen insgesamt die Dynamik, wie sich Anonymität auf das Verhalten und die soziale Interaktion im Web auswirkt.

Deindividuationstheorie

In ihrem Paper verweist Christopherson [2] auf Zimbardos Deindividuationstheorie, die besagt, dass in Gruppen, in denen der Einzelne nicht als Individuum gesehen oder beachtet wird, die inneren Hemmschwellen für verschiedene Handlungen sinken. Zimbardo betont die Rolle der Anonymität bei der Schaffung eines deindividuierten Zustands, welcher zu einer Verringerung der Selbstbeobachtung und Selbsteinschätzung führt, was wiederum eine Schwächung der verinnerlichten Kontrollen wie Schuld und Scham und eine Zunahme ungehemmten Verhaltens zur Folge hat [2, p. 3044]. Weiterhin merkt Christopherson an, dass einige Forscher die Idee unterstützen, anonyme Menschenmengen erzeugten einen deindividuierten Zustand, der zu antisozialem Verhalten führt, während andere argumentieren, dass antisoziales Verhalten eher mit der Selbstwahrnehmung eines Individuums zusammenhängt [2, p. 3045].

Equalization Hypothesis

In Bezug auf die Equalization Hypothesis (Gleichstellungshypothese) erörtert Christopherson [2], wie CMC das soziale Spielfeld ebnet, indem sie physische Merkmale wie Geschlecht, Rasse und Alter herausfiltert, die bei Interaktionen von Angesicht zu Angesicht eine wichtige Rolle spielen [2, pp. 3045-3046]. Diese Hypothese besagt, dass CMC soziale Ungleichheiten und Stereotypen abbauen und eine gleichberechtigtere Kommunikation ermöglichen sollte, insbesondere für Personen, die traditionell einen niedrigeren Status haben [2, pp. 3045-3046]. Christopherson weist jedoch auch auf Einschränkungen und gemischte Ergebnisse von Studien zur Gleichstellungshypothese hin [2, p. 3046]. Entgegen dieser deuten neuere Forschungsergebnisse darauf hin, dass CMC nicht unbedingt zu mehr Gleichheit in der Kommunikation führt. Traditionelle Geschlechterrollen und -erwartungen können in CMC-Umgebungen fortbestehen, insbesondere wenn die Identitäten der Teilnehmer nicht vollständig anonym sind [2, pp. 3046-3047].

SIDE-Theorie

Die SIDE-Theorie (Social Identity Model of Deindividuation Effects), wie sie von Christopherson [2, pp. 3047-3048] erläutert wird, ist eine Neuinterpretation der klassischen Deindividuationstheorie, die den Schwerpunkt auf situative Variablen in sozialen Situationen legt. Diese Theorie besteht aus zwei Komponenten: einer kognitiven Komponente, die sich darauf konzentriert, wie Gruppendynamik und individuelles Verhalten innerhalb von Gruppen durch Anonymität vermittelt werden, und einer strategischen Komponente, die den absichtlichen Einsatz von Anonymität in CMC beinhaltet [2, pp. 3047-3048].

Der kognitive Aspekt, der von Spears und Lea vorgeschlagenen SIDE-Theorie besagt, dass die Anonymität im CMC die Wirkung sozialer Normen verstärkt, wenn die soziale Identität stark ist. Sie sagt unterschiedliche soziale Interaktionsprozesse voraus, die vom Grad der Anonymität innerhalb einer Gruppe abhängen [2, p. 3048]. Auf der strategischen Seite geht die Theorie davon aus, dass Menschen die Anonymität im CMC nutzen, um ihre eigenen Kommunikationsziele zu erreichen. Zum Beispiel könnten Minderheitengruppen Anonymität nutzen, um Ansichten zu äußern, die den Normen der Mehrheitsgruppe zuwiderlaufen. Die Forschung hat gezeigt, dass Männer und Frauen die Anonymität in CMC unterschiedlich nutzen, wobei Männer versuchen, die Anonymität zu reduzieren, während Frauen sie aufrechterhalten, um die Machtdynamik auszugleichen [2, pp. 3048-3049].

Adaptive Structuration Theory

Christopherson [2] diskutiert die Adaptive Structuration Theory in Bezug auf die soziale Nutzung von Technologie, insbesondere im Zusammenhang mit der Anonymität in CMC. Sie geht von zwei Prozessen bei der Nutzung von Technologien aus: dem von den Entwicklern beabsichtigten Zweck und den entstehenden Nutzungen, die sich aus der Interaktion der Menschen mit der Technologie ergeben und

die von der ursprünglichen Absicht drastisch abweichen können [2, pp. 3049-3050]. Das Paper betont die strategische Komponente der SIDE-Theorie bei der Bestimmung der Folgen von Anonymität in CMC. Dieser Aspekt der SIDE-Theorie hebt die duale Natur der Anonymität hervor, die entweder zu prosozialem oder antisozialem Verhalten führen kann. Das Ergebnis hängt davon ab, wie der Einzelne die Anonymität nutzt, was je nach persönlichen Ansichten und sozialen Normen unterschiedlich sein kann. Die SIDE-Theorie gilt als wichtiger und einflussreicher Rahmen für das Verständnis der Anonymität in Internet-Interaktionen [2, p. 3051].

2.5 Dark Web

Mit keinem Bereich des Internets wird Cyberkriminalität so stark verbunden wie mit dem Dark Web. Es bietet eine nahezu vollständige Anonymität und ist dementsprechend beliebt bei Nutzern mit sträflichen Absichten. Doch dieser Schattenseite stehen viele positive Aspekte gegenüber. Im Folgenden soll das Dark Web, das Tor-Netzwerk und die Regulierung beider Technologien auf Grundlage dreier wissenschaftlicher Artikel betrachtet werden.

2.5.1 Funktionsweise

Mitte der 1990er Jahre entwickelte das „Naval Research Laboratory“, das Forschungslabor der US Navy, eine Netzwerktechnik mit dem Namen „Onion Routing“. Das Ziel dieser Unternehmung war die Gewährleistung von Anonymität bei der Nachrichtenübermittlung von militärischem Personal im Ausland [8, p. 27]. Für diese Anonymität musste die Technik jedoch der Öffentlichkeit zur Verfügung gestellt werden, andernfalls könnte jede Nachricht über dieses Netzwerk einem kleinen Kreis zugeordnet werden [6, p. 2131].

Die zugrundeliegende Idee des Onion Routing ist die Weitergabe einer Webseitenanfrage über eine bestimmte Anzahl an Knoten, sogenannte „Relays“. Diese werden nach einem Zufallsverfahren ausgewählt und reichen die Anfrage an das jeweils nächste Relay weiter. Dabei kennt jeder Knoten lediglich seine beiden Nachbarn. Der Ausgangsknoten, auch Exit-Relay genannt, gibt die Anfrage an den Server weiter. Der Server erfährt nur die IP-Adresse des Exit-Relays, nicht jedoch die Adresse des ursprünglichen Absenders [7, p. 2]. Zusätzlich wird jede Nachricht zwischen den Relays mit einem eigenen Schlüssel verschlüsselt. Diese Vielschichtigkeit an Verschlüsselungen führt zu dem Namen der Zwiebel, dessen Inhalt nur der Absender wieder entschlüsseln kann. Hierdurch sind die Daten vor dem Mitlesen durch Dritte geschützt [6, p. 2133].

Für den Zugriff auf Seiten des Dark Webs wird das Onion Routing vorausgesetzt, da nur Anfragen der Exit-Relays angenommen werden. Am weitesten verbreitet ist der Tor-Browser, es existieren jedoch auch andere Browser mit dieser Funktionalität. Die Browser sind nicht auf Zugriffe im Dark Web beschränkt, sondern können auch für das anonyme Surfen im „Surface Web“ sowie dem „Deep Web“ genutzt werden, dem Internet wie wir es täglich nutzen. Lediglich 1,5% der Nutzer des Tor-Browsers rufen Seiten aus dem Dark Web ab, hauptsächlich bilden der Schutz der Privatsphäre und die persönlichen Sicherheit Gründe für die Nutzung des Onion Routing [8, p. 28].

2.5.2 Vor- und Nachteile des Tor-Netzwerks

Das Tor-Netzwerk gewährleistet den Nutzern höchste Anonymität. Dies kann sowohl im positiven Sinne als auch für schändliche bis sträfliche Aktivitäten genutzt werden. In Abschnitt 2.4.3 wurden bereits die politischen Aspekte der Anonymität beleuchtet. Gerade in totalitäreren Staaten wird das Tor-Netzwerk sowie das Dark Web für den Ausdruck der Meinungsfreiheit sowie der Umgehung von Zensuren genutzt. Für politische Aktivisten, Reformer und Journalisten ist es ein essenzielles Werkzeug, um der staatlichen oder unternehmerischen Überwachung und Verfolgung zu entgehen [7, pp. 4-5].

Dem steht jedoch der Missbrauch der Anonymität entgegen: Drogenhandel, Verbreitung von Kinderpornografie, Hacking-Aufträge, Waffenhandel und viele weitere illegale Arten der Kriminalität lassen sich im Dark Web finden. Der stetige Wechsel von Server-Adressen sowie den Namen der Seiten

solcher Dienste erschweren ein konsequentes Vorgehen der Polizei gegen dieses Phänomen, während die Nutzer ebenfalls unbekannt bleiben [6, pp. 2140-2143].

2.5.3 Bekämpfung der Cyberkriminalität

Die polizeiliche Arbeit im Dark Web ist durch die Anonymität der Nutzer sowie die angesprochene Kurzlebigkeit der Webseiten kompliziert, jedoch nicht unmöglich. In einer Reihe von Gegenbeispielen konnten einige Straftäter gefasst und verurteilt werden. Der berühmteste Fall betrifft die Seite „Silk Road“, ein Marktplatz für illegale Produkte und Dienstleistungen. Der Betreiber dieser Seite konnte durch ein fehlerhaft konfiguriertes „Captcha“ nach Island zurückverfolgt und verhaftet werden. Außerdem wurde die Seite abgeschaltet, was jedoch eine Vielzahl an neuen Seiten desselben Zwecks nach sich zog [8, p. 30].

Von polizeilicher Seite wird durch den hohen Aufwand und die fehlenden Kapazitäten im Kampf mit der Cyberkriminalität im Dark Web häufig der Einbau von Kontrollfunktionen gefordert. Dies soll entweder in Form von Hintertüren geschehen, durch welche Nutzer zurückverfolgt werden könnten, oder durch die Speicherung von Daten, welche Nutzer auf welche Seiten zugegriffen haben. Beide Aspekte sind jedoch mit Verwundbarkeiten des Tor-Netzwerks sowie einer Deanonymisierung verbunden [7, p. 7].

Die drei recherchierten Artikel sind sich darin einig, dass die Cyberkriminalität bekämpft, dabei jedoch die Anonymität der unschuldigen Nutzer geschützt werden muss. Nach Chertoff ist die Verfolgung der Betreiber nicht die Lösung für dieses Problem. Auf jede aus dem Netz genommene Seite folgen etliche neue Seiten, die den frei gewordenen Platz einnehmen wollen. Stattdessen sollten die Nutzer identifiziert werden und ein Verständnis geschaffen werden, dass illegale Aktivitäten im Dark Web nicht unentdeckt bleiben. Somit würde die Cyberkriminalität zurückgehen, während die Anonymität bewahrt werden würde [8, p. 36].

Das Dark web bietet auch Vorteile für die Polizeiarbeit: Es können illegale Seiten besucht werden, ohne dass Spuren hinterlassen werden. Dies ermöglicht außerdem Undercover Operationen, durch welche die Polizei unbemerkt Informationen sammeln kann. Des Weiteren werden anonyme Tipps häufiger über das Dark Web publiziert, da hier die höchste Form der Anonymität gewährleistet wird [6, p. 2154].

2.5.4 Das Dark Web Dilemma

Das Tor-Netzwerk wird insbesondere in liberalen und totalitären Staaten genutzt. Liberal ausgerichtete Länder erlauben eine uneingeschränkte Nutzung des Netzwerks, was viele Nutzer nach sich zieht. Mit der Androhung von Strafen sinkt diese Zahl deutlich, bis der Punkt erreicht wird, an welchem sich Menschen ungeachtet der Konsequenzen gezwungen fühlen, das Tor-Netzwerk und das Dark Web zu nutzen, um ihre politische Freiheit ausleben zu können [7, pp. 6-7].

Die illegalen Aktivitäten lassen sich am häufigsten in den liberalen Ländern verorten. Es sind allerdings auch die liberaleren Staaten, durch welche das Tor-Netzwerk größtenteils weiterentwickelt und gehostet wird. Die Forderungen nach Einschränkungen oder Eingriffsmaßnahmen im Dark Web stammen dementsprechend aus den Ländern, welche das Netzwerk in seiner jetzigen Form ermöglichen. Gerade Nutzer aus Staaten mit wenigen politischen Rechten profitieren vom Angebot der Anonymität, sind jedoch abhängig davon, dass die liberaleren Staaten den Preis einer höheren Kriminalität bezahlen, damit das Netzwerk weiterhin besteht. Diese Situation wird von Jardine als „Dark Web Dilemma“ bezeichnet [7, pp. 7-8].

Um die positiven Aspekte des Tor-Netzwerks und des Dark Webs auch weiterhin bewahren zu können, ist eine Alternative zur Bekämpfung der Cyberkriminalität erforderlich. Anstelle von strukturellen Änderungen des Netzwerks sollte laut Jardine die Polizeiarbeit in diesem Bereich verbessert werden. Durch Training im Umgang mit der Materie, mehr Koordination von polizeilichen Behörden, optimierter Kommunikation sowie höheren Kapazitäten soll die Cyberkriminalität effektiver zurückgedrängt werden [7, p. 10].

Ein weiterer wichtiger Aspekt ist die internationale Zusammenarbeit. Das Internet und ebenso das Dark Web agieren auf internationaler Ebene und Straftäter müssen durch internationale Zusammenarbeit gefasst werden. Daher muss ein gemeinsamer Konsens dafür geschaffen werden, was im Dark Web verfolgt werden muss und wie die polizeilichen Behörden verschiedener Staaten kooperieren können [8, p. 32].

3 Fazit

In diesem Kapitel stellen wir unsere eigene begründete Bewertung unserer recherchierten Ergebnisse vor.

3.1 Soziale Aspekte

Anhand der Rechercheergebnisse lässt sich zusammenfassen, dass Anonymität im Web eine ambivalente Rolle spielt. Die vorgestellten Studien von Christopherson [2] stellen klar heraus, dass Anonymität positive Auswirkungen auf das psychische Wohlbefinden haben kann und die Möglichkeit zur Selbstbestimmung in Bezug auf den Grad der Privatsphäre dabei ein entscheidender Faktor ist. Auch kann Anonymität einen positiven Effekt zur Selbstoffenbarung haben [9]. In der Kommunikation in Gruppen bietet die Anonymität im Web ebenso einige Vorteile. Jedoch ist der Schutz vor Zensur und politischer Verfolgung sowie die Stärkung von Presse- und Meinungsfreiheit ein entscheidender Vorteil der Anonymität, insbesondere in Ländern mit autoritären Regimen. Damit kann Anonymität als wichtiges Werkzeug zur Stärkung der Demokratie und zum Schutz der Menschenrechte betrachtet werden [3, 6].

Jedoch ist auch anzuerkennen, dass Anonymität die Tür für die Verbreitung von Falschinformationen und die Begehung von Straftaten öffnet, was potenziell die Demokratie untergraben kann [7]. Genauso konzentrieren sich viele Studien auf die negativen Aspekte der Anonymität, wie z.B. verstärktes aggressives Verhalten, die Förderung von isolierendem Verhalten und gefährliche Gruppendynamiken [2].

In diesem Spannungsfeld zwischen positiven und negativen Aspekten ist es entscheidend, eine ausgewogene Perspektive einzunehmen und darüber nachzudenken, wie die Vor- und Nachteile von Anonymität in verschiedenen Kontexten sorgfältig abgewogen und reguliert werden können. Zwar überwiegen für das Individuum die Vorteile, in Gruppen führt Anonymität jedoch vielfach zu negativem Verhalten. Zur Wahrung der Menschenrechte (also eine noch größere Gruppenebene) überwiegen wiederum klar die Vorteile.

3.1.1 Auswertung und Bewertung der Theorien

Ein Blick auf die recherchierten Theorien hinter den sozialen Auswirkungen ergibt ebenfalls ein differenziertes Bild. Zimbardos Deindividuationstheorie, welche nahelegt, dass Anonymität in Gruppen zu einer Verringerung der Selbstkontrolle und einer Freisetzung ungehemmten Verhaltens führen kann, wurde in den Anfängen der CMC entwickelt wurde und gilt inzwischen als teilweise überholt [2, pp. 3044-3045]. Neuere Forschungen zeigen, dass die Wirkung von Anonymität auf das Verhalten komplexer ist und nicht zwangsläufig zu deindividuiertem Verhalten führt [2, pp. 3044-3045]. Die Equalization Hypothesis, welche davon ausgeht, dass CMC das soziale Spielfeld ebnet, indem sie physische Merkmale wie Geschlecht, Rasse und Alter herausfiltert, gilt ebenfalls als teilweise überholt [2, pp. 3045-3047]. Aufbauende Studien zeigen, dass CMC nicht automatisch zu mehr Gleichheit führt und dass traditionelle Geschlechterrollen und -erwartungen fortbestehen können [2, pp. 3046-3047]. Die SIDE-Theorie, eine Neuinterpretation der Deindividuationstheorie, betont, dass Anonymität in CMC die Wirkung sozialer Normen verstärken kann, was zu einer stärkeren Gruppendynamik führt [2, pp. 3047-3049]. Gleichzeitig impliziert die Theorie, dass Anonymität zu einer Polarisierung und Verstärkung von Gruppenideologien führen kann. Die SIDE-Theorie bleibt in ihrer Anwendung relevant, wurde jedoch weiterentwickelt, um die sich ändernden Dynamiken des Internets und die Vielfalt der Online-

Interaktionen besser zu berücksichtigen. Die Adaptive Structuration Theory geht bezüglich Anonymität in CMC davon aus, dass die duale Natur der Anonymität sowohl zu prosozialem als auch antisozialem Verhalten führen kann, abhängig davon, wie der Einzelne die Anonymität nutzt [2, pp. 3049-3051]. Sie bleibt weitgehend relevant, wird jedoch kontinuierlich angepasst, um den raschen technologischen Wandel und die Entwicklung neuer Kommunikationsformen im Web zu reflektieren [2, pp. 3049-3051].

Die Evaluation der vorgestellten Theorien zeigt, dass die sozialen Auswirkungen von Anonymität im Web ein facettenreiches und sich stetig weiterentwickelndes Forschungsfeld darstellen. Insbesondere die Erkenntnis, dass Anonymität nicht zwangsläufig zu deindividuiertem oder egalisiertem Verhalten führt, verdeutlicht die Komplexität der menschlichen Interaktion im digitalen Raum. Insgesamt legen diese Theorien nahe, dass die Wirkung von Anonymität im Web sowohl positive als auch negative Konsequenzen haben kann, abhängig von verschiedenen Faktoren wie Kontext, sozialen Normen und der individuellen Nutzung.

3.2 Technische Identifikation

Es gibt zahlreiche Tools, mit denen Anonymität im Web erreicht werden kann, oder der Grad an Anonymität zumindest gesteigert werden kann. Dazu gehört beispielsweise der Tor-Browser, der die Möglichkeit bietet, das Tor-Netzwerk zu benutzen. Schwachstellen des Netzwerkes sind jedoch die Ein- und Ausgangsknoten, falls diese überwacht werden, ist keine Anonymität gegeben (vgl. auch [6]). VPNs (Virtual Private Networks) tragen auch zu einer erhöhten Anonymität bei, jedoch nur eingeschränkt. Durch sie ist ein Tracking im lokalen Netzwerk oder durch ISPs nur noch eingeschränkt möglich. Außerdem wird die echte IP-Adresse verschleiert [11]. Ein VPN ist jedoch keine vollständige Lösung zum Erreichen von Anonymität. Daneben gibt es auch zahlreiche Browsererweiterung, die Werbung und (unsichtbare) Tracker sowie Cookies blockieren.

Um Anonymität im Web zu erreichen, sind jedoch viele verschiedene Tools nötig. Nur beim Einsatz verschiedenster Tools kann ein gewisser Grad an Anonymität erreicht werden. Zusätzlich muss der Nutzer jedoch auch identifizierende Informationen zurückhalten. Um eine vollständige Anonymität nicht nur gegenüber Unternehmen und Privatpersonen, sondern auch vor staatlichen Akteuren zu bewahren, sind allerdings noch deutlich weiterreichende Maßnahmen nötig (vgl. auch [6], [5], [7] oder [4]).

3.3 Dark Web

Mit der Technologie des Tor-Netzwerks und dem damit einhergehenden Dark Web wird die Spitze der Anonymität erreicht. Nutzer können nur unter sehr hohem Aufwand identifiziert werden und übermittelte Daten werden durch eine Vielzahl an Verschlüsselungen vor dem Zugriff durch Dritte geschützt [8] [6].

Diese Höhe der Anonymität lässt jedoch positive wie auch negative Aspekte in Erscheinung treten. Auf der positiven Seite wird der Allgemeinheit ein Werkzeug bereitgestellt, mit welchem die Privatsphäre sowie die eigene Sicherheit gewährleistet wird. Gerade in totalitären Staatsformen bietet das Tor-Netzwerk einen Weg für die Auslebung demokratischer Aspekte, wie der Meinungsfreiheit und dem Umgehen von Zensur. Die negative Seite birgt ein großes Repertoire an Cyberkriminalität, welchem aktuell nur in Ausnahmefällen begegnet werden kann. Von polizeilicher Seite wird daher der Einbau von Hintertüren oder die Aufzeichnung von übermittelten Daten der Nutzer gefordert. Dies würde jedoch dem grundlegenden Paradigma des Tor-Netzwerks widersprechen und eine Deanonymisierung zur Folge haben [8] [7].

Mit dem Wachstum des Internets wurden und werden immer mehr Aktivitäten online ausgeübt. Dies schließt auch illegale Aktivitäten mit ein, und ebenso muss auch die polizeiliche Verfolgung dieser Straftaten in das Internet transferiert werden [7].

Die polizeiliche Grundlage für die Bekämpfung der Cyberkriminalität ist jedoch nicht weit genug entwickelt, um die aktuelle Kriminalität im Dark Web effizient auf Nutzer zurückführen zu können. Im

Fall einiger Seiten konnten Erfolge erzielt werden, jedoch nicht in einem Maß, welches mit der Strafverfolgung in der physischen Welt mithalten könnte. Hierfür sind Weiterbildungen, bessere Kommunikation und Koordination sowie mehr Kapazitäten notwendig [7] [8].

Ein weiteres Hindernis ist die Zusammenarbeit von Behörden auf internationaler Ebene. Das Dark Web agiert international, Daten, Server und Nutzer sind über viele Staaten verteilt. Allerdings läuft die Zusammenarbeit sehr stockend, auch aufgrund von unterschiedlichen Gesetzeslagen in den Ländern. Für eine bessere Kooperation muss ein gemeinsamer Konsens für die Handhabung mit Cyberkriminalitätsfällen geschaffen werden [8].

Den wohl bekanntesten Fall der Bekämpfung von Cyberkriminalität stellt das Aufspüren des Betreibers der Seite „Silk Road“ dar, einem Marktplatz für illegale Güter und Dienstleistungen. Der Betreiber wurde zu einer lebenslänglichen Haftstrafe ohne Bewährung verurteilt und die Seite vom Netz genommen [8].

Dies hatte jedoch zur Folge, dass sowohl neue Seiten, insbesondere Silk Road 2.0 und später Silk Road 3.0, an dieser frei gewordenen Stelle erschienen, als auch dass die Betreiber höhere Sicherheitsmaßnahmen ergriffen. Ein ständiger Wechsel der Namen sowie Adressen der Seiten begann, durch welchen sich die Server schwerer lokalisieren lassen [8].

Ein ähnliches Phänomen ist auch mit dem gesamten Dark Web denkbar. Sollten Hintertüren oder andere Formen der Deanonymisierung eingebaut werden, so ist es durchaus denkbar, dass eine neue Technologie den Platz des Dark Webs einnimmt, welche möglicherweise nicht so leicht zu infiltrieren ist wie das Dark Web.

Das Tor-Netzwerk ist in erster Linie ein Werkzeug, welches in der Nutzung keine Straftat mit sich führt, das Gegenteil ist eher der Fall: Der Tor-Browser wird hauptsächlich für das anonyme Surfen im legalen Bereich des Internets genutzt. Man sollte sich darauf konzentrieren, gezielt Straftäter zu identifizieren, anstatt das Werkzeug selbst zu verbieten oder seine Integrität zu untergraben, was zur Gefährdung der Anonymität führen könnte [8] [7] [6].

Um dieses Ziel zu erreichen, ist es erforderlich, dass die polizeiliche Arbeit sich gezielt auf die kriminellen Seiten konzentriert, die Nutzer identifiziert und gleichzeitig die Botschaft sendet, dass Kriminalität im Dark Web zurückverfolgt und bestraft wird. Auf diese Weise bleibt die Anonymität unschuldiger Nutzer gewahrt, während gleichzeitig die Cyberkriminalität rückläufig wird.

4 Ausblick

Diese Arbeit betrachtet ein breites Spektrum an Aspekten rund um die Anonymität im Web, von denen viele wichtige Fragen offenlassen. In diesem Abschnitt sind einige der signifikanten zukünftigen Forschungsrichtungen zusammengetragen.

4.1 Zukünftige Arbeiten in Hinblick auf soziale Aspekte

Für die künftige Forschung ist eine tiefere Erforschung des nuancierten Konzepts der Anonymität als Kontinuum und nicht als binärer Zustand von wesentlicher Bedeutung. Solche Studien sollten die Entwicklung und Validierung standardisierter Messgrößen für die wahrgenommene Anonymität beinhalten, um konsistentere und vergleichbare Ergebnisse in verschiedenen Studien zu ermöglichen.

Darüber hinaus besteht die Möglichkeit, das Zusammenspiel kultureller und politischer Faktoren bei den Motivationen für Anonymität zu untersuchen. Vergleichende Studien über verschiedene kulturelle und politische Kontexte hinweg könnten aufzeigen, wie diese Faktoren die Praktiken der Online-Anonymität in einzigartiger Weise beeinflussen. Dies ist besonders wichtig für die Untersuchung der geschlechtsspezifischen Unterschiede bei der Nutzung und Wahrnehmung von Anonymität im Internet, wobei zu untersuchen ist, wie Faktoren wie Sicherheit, soziale Machtdynamik und kulturelle Normen diese Unterschiede beeinflussen.

Weiterhin kann die Anwendung und Überprüfung von Theorien wie der Adaptive Structuration Theory im Kontext der SIDE-Theorie in verschiedenen Online-Umgebungen wertvolle Erkenntnisse liefern. Dazu gehört die Untersuchung, wie sich Anonymität auf das Gruppenverhalten und die soziale Machtdynamik in Online-Gemeinschaften auswirkt, wobei der Schwerpunkt auf bestimmten Online-Plattformen oder Interaktionsarten wie sozialen Medien, Foren und virtuellen Räumen liegt. Schließlich sind auch Längsschnittstudien, welche die Entwicklung von Anonymitätspraktiken und ihre Auswirkungen im Laufe der Zeit untersuchen, für das Verständnis der sich verändernden Landschaft der Online-Kommunikation und ihrer sozialen Auswirkungen von entscheidender Bedeutung.

4.2 Aufbauende Arbeiten im Bereich des Dark Webs

Zukünftige Arbeiten werden auch weiterhin das zweischneidige Schwert der Anonymität des Dark Webs diskutieren und den Kampf gegen die Cyberkriminalität mit den positiven Aspekten des Tor-Netzwerks vergleichen.

Im Fall der Umstrukturierung von polizeilicher Arbeit im Dark Web können Artikel über neue polizeiliche Strategien und Taktiken erwartet werden, beispielsweise zur Integration neuer Technologien in der Strafverfolgung oder von Kooperationsmaßnahmen internationaler Behörden. Sollte stattdessen in der Zukunft das Dark Web in irgendeiner Weise deanonymisiert werden, so wird eine Reihe an Arbeiten diese Änderung ausführlich diskutieren.

Soziologische Auswirkungen oder Nutzerverhalten im Dark Web wären weitere spannende Forschungsthemen, allerdings lassen sich solche Daten im Kontext des Dark Webs nur schwer erheben. Die meisten Nutzer wollen anonym bleiben und sich nicht der Öffentlichkeit preisgeben, was wissenschaftliche Arbeiten zu diesem Thema nicht begünstigt.

Literaturverzeichnis

[1] Statista, „Attitudes and actions of online users in the United States regarding online privacy as of 3rd quarter 2022," Februar 2023. [Online]. Verfügbar: https://www.statista.com/statistics/1424653/online-adults-attitudes-data-privacy-us/. [Zugriff am 7. Januar 2024].

[2] K. M. Christopherson, „The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog"," in *Computers in Human Behavior,* Bd. 23, Nr. 6, pp. 3038-3056, 2007. DOI.

[3] J. Palme und M. Berglund, „Anonymity on the Internet," 2002. [Online]. Verfügbar: https://people.dsv.su.se/~jpalme/society/anonymity.pdf. [Zugriff am 14. November 2023].

[4] K. Ruogu, S. Brown und S. Kiesler, „Why Do People Seek Anonymity on the Internet? Informing Policy and Design," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2657–2666, New York, 2013. DOI.

[5] S. Englehardt, D. Reismann, C. Eubank, P. Zimmermann, J. Mayer, A. Narayanan und E. W. Felten, „Cookies That Give You Away: The Surveillance Implications of Web Tracking," in *Proceedings of the 24th International Conference on World Wide Web*, pp. 289–299, Genf, 2015. DOI.

[6] S. Kaur und S. Randhawa, „Dark Web: A Web of Crimes," in *Wireless Personal Communications,* Bd. 112, pp. 2131-2158, 2020. DOI.

[7] E. Jardine, „The Dark Web Dilemma: Tor, Anonymity and Online Policing," in *Global Commission on Internet Governance Paper Series,* Bd. 21, 2015. DOI.

[8] M. Chertoff, „A public policy perspective of the Dark Web," in *Journal of Cyber Policy,* Bd. 2, Nr. 1, pp. 26-38, 2017. DOI.

[9] C. Clark-Gordon, N. Bowman, A. Goodboy und A. Wright, „Anonymity and Online Self-Disclosure: A Meta-Analysis," in *Communication Reports,* Bd. 32, Nr. 2, pp. 98-111, 2019. DOI.

[10] R. Boyd und L. K. Field, „Blind Injustice: Theorizing Anonymity and Accountability in Modern Democracies," in *Polity,* Bd. 48, Nr. 3, pp. 332-358, 2016. DOI.

[11] Kaspersky, „What is VPN? How It Works, Types of VPN," [Online]. Verfügbar: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn. [Zugriff am 22. Dezember 2023].

[12] Focus, „Anteil der Websites im Darknet nach Kategorien im Jahr 2016," 6. August 2016. [Online]. Verfügbar: https://de.statista.com/statistik/daten/studie/588281/umfrage/anteil-der-websites-im-darknet-nach-kategorien/. [Zugriff am 4. Januar 2024].

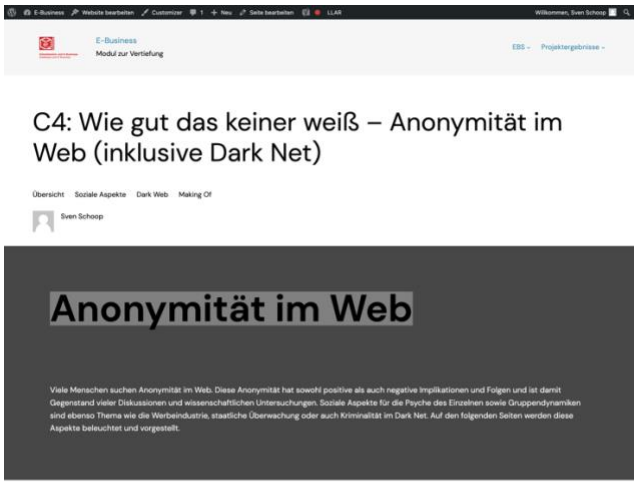
[13] Focus, „Anzahl der täglichen Nutzer des Tor-Netzwerks in ausgewählten Ländern weltweit im Jahr 2016 (in 1.000)," 6. August 2016. [Online]. Verfügbar: https://de.statista.com/statistik/daten/studie/588309/umfrage/anzahl-der-taeglichen-nutzer-des-tor-netzwerks-nach-laendern-weltweit/. [Zugriff am 6. Januar 2024].

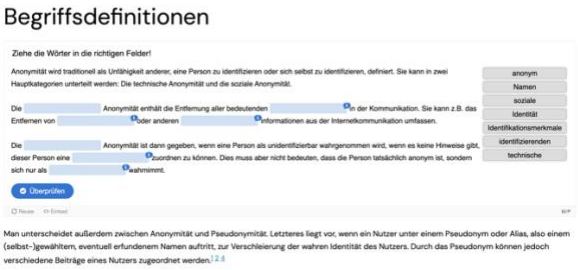
Abbildungsverzeichnis

Anhang

Ausdrucke Websites:

- Überblick
- Soziale Aspekte
- Dark Web





Technische Identifikation

Die (eindeutige) Identifikation eines Nutzers bzw. die Aufhebung seiner Anonymität kann durch verschiedene Daten und deren Kombination erfolgen. Dazu gehören u.a. Name, Aufenthaltsort, Pseudonyme, die Rückschlüsse auf die wahre Identität ermöglichen, Verhaltensmuster, Mitgliedschaft in einer sozialen Gruppe, Informationen/Gegenstände oder Fähigkeiten, die auf die persönliche Charakteristik hinweisen. Außerdem auch technische Daten, wie z.B. die IP-Adresse.[1] Im Folgenden werden verschiedene Arten und Weisen vorgestellt, wie eine technische Identifikation gelingen kann.

Cookies

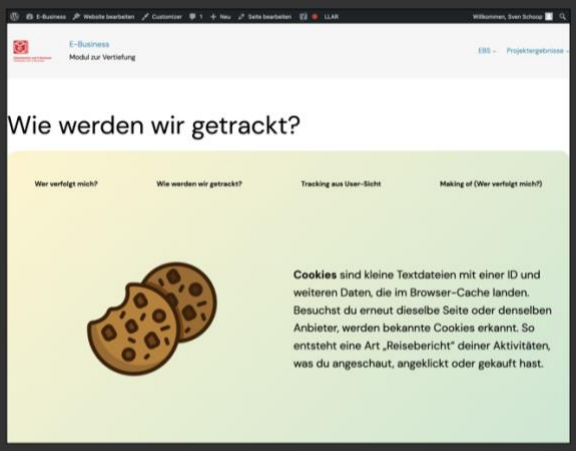
Der Einsatz von Third-Party Tracking-Cookies kann sogar zur Massenüberwachung genutzt werden. Cookies sind kleine Textdateien, die von Webseiten im Browser gesetzt werden können. Verwenden mehrere Webseiten den selben Tracking-Cookie lassen sich Besuche verschiedenster Webseiten auf den gleichen Nutzer zurückverfolgen, auch wenn sich z.B. die IP-Adresse ändert.[2]

ISPs

ISPs (Internet Service Provider, also Internetanbieter) besitzen viele Möglichkeiten Nutzer eindeutig zu identifizieren. Durch die Bereitstellung der Internetverbindung nehmen die ISPs die Zuordnung der IP-Adressen zu den Kunden, die dem ISP mit Klarnamen und Adresse bekannt sind, vor. Außerdem wird der gesamte Netzwerkverkehr zuerst über die Infrastruktur des ISPs geroutet, bevor das eigentliche Internet erreicht wird.[3,4]

Gruppe Cx hat das Thema *Wer verfolgt mich? – Die Krux mit dem Tracking* bearbeitet, in dem tiefergreifend auf Web-Tracking eingegangen wird.

Gruppe Cx – Web-Tracking



Tools Tools Tools

Es gibt allerdings auch einige Tools, mit denen sich eine gewissen Anonymität im Web erreichen lässt.[2] Im Folgenden seien einige exemplarisch dargestellt.

Tor und das Dark Net

Quellen

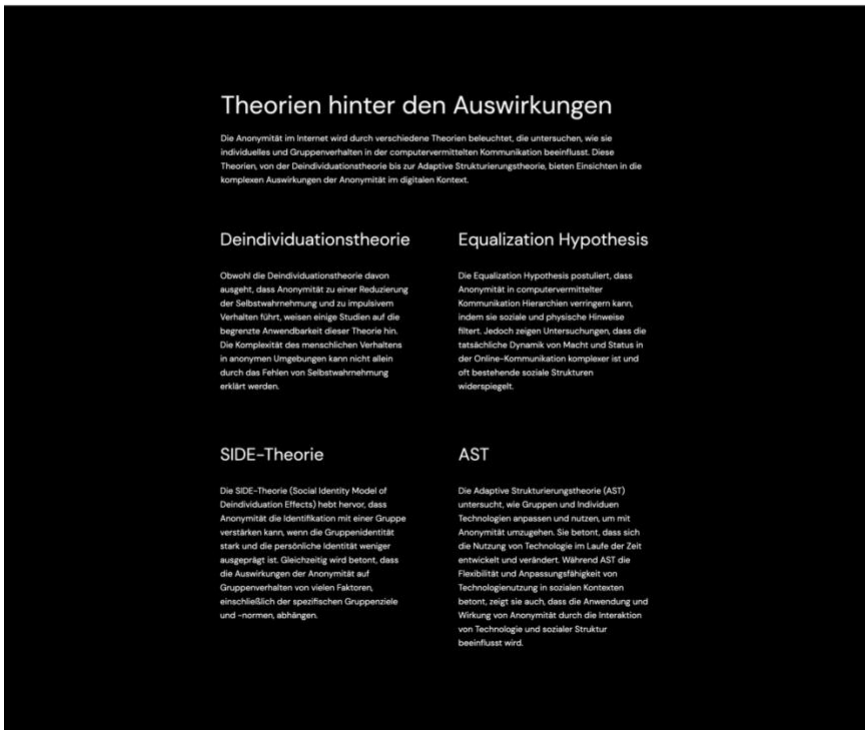
1. Christopherson, K.M.: The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog". In: Computers in Human Behavior, Volume 23, Issue 6, 2007, S. 3038–3056. DOI.
2. Ruoqu, K., Brown, S., Kiesler, S.: Why Do People Seek Anonymity on the Internet? Informing Policy and Design. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, S. 2657–2666. Association for Computing Machinery, New York 2013. DOI.
3. Englehardt, S., Reisman, D., et. al.: Cookies That Give You Away: The Surveillance Implications of Web Tracking. In: Proceedings of the 24th International Conference on World Wide Web, S. 289–299. International World Wide Web Conferences Steering Committee, Genf 2015. DOI.
4. Palme, J., Berglund, M.: Anonymity on the Internet, 2002. https://people.dsv.su.se/~jpalme/society/anonymity.pdf, Abgerufen am: 14.11.2023.

Bildquellen


E-Business
Modul zur Vertiefung
EBS
Projektergebnisse
Soziale Aspekte
Übersicht
Soziale Aspekte
Dark Web
Making Of
Luca Selinski
Soziale Aspekte
von Anonymität im Web

Auswirkungen auf die Kommunikation
Anonymität im Internet beeinflusst die Kommunikation sowohl auf individueller als auch auf Gruppenebene. Persönlich ermöglicht sie freieren Ausdruck, birgt aber Risiken für unverantwortliches Verhalten. In Gruppen fördert sie Kohäsion, kann aber auch zu Polarisierung führen. Dieser Abschnitt beleuchtet diese Dualität.
Auf persönlicher Ebene
Anonymität schützt Privatsphäre und fördert freie Meinungsäußerung, kann aber zu unverantwortlichem Verhalten und Aggression führen. Sie ermöglicht Ausdruck ohne Furcht vor sozialer Bewertung, birgt aber auch Risiken für soziale Missverständnisse.
Auf Gruppenebene
Anonymität in Gruppen fördert Gruppenkonformität und Polarisierung. Sie kann zu verstärkter Gruppenidentität führen, gleichzeitig aber auch die Verantwortlichkeit und individuelle Rechenschaftspflicht mindern.


Kernaussagen zu den Auswirkungen
Wähle jeweils die korrekte Aussage, um dich selbst zu testen:
Fortschritt: 0/3
Anonymität unterdrückt generell die freie Meinungsäußerung, da sie zu einer erhöhten Angst vor sozialer Bewertung führt.
Anonymität kann die freie Meinungsäußerung fördern, indem sie die Angst vor sozialer Bewertung reduziert.


Theorien hinter den Auswirkungen
Die Anonymität im Internet wird durch verschiedene Theorien beleuchtet, die untersuchen, wie sie individuelles und Gruppenverhalten in der computervermittelten Kommunikation beeinflusst. Diese Theorien, von der Deindividuationstheorie bis zur Adaptive Strukturierungstheorie, bieten Einsichten in die komplexen Auswirkungen der Anonymität im digitalen Kontext.
Deindividuationstheorie
Obwohl die Deindividuationstheorie davon ausgeht, dass Anonymität zu einer Reduzierung der Selbstwahrnehmung und zu impulsivem Verhalten führt, weisen einige Studien auf die begrenzte Anwendbarkeit dieser Theorie hin. Die Komplexität des menschlichen Verhaltens in anonymen Umgebungen kann nicht allein durch das Fehlen von Selbstwahrnehmung erklärt werden.
Equalization Hypothesis
Die Equalization Hypothesis postuliert, dass Anonymität in computervermittelter Kommunikation Hierarchien verringern kann, indem sie soziale und physische Hinweise filtert. Jedoch zeigen Untersuchungen, dass die tatsächliche Dynamik von Macht und Status in der Online-Kommunikation komplexer ist und oft bestehende soziale Strukturen widerspiegelt.
SIDE-Theorie
Die SIDE-Theorie (Social Identity Model of Deindividuation Effects) hebt hervor, dass Anonymität die Identifikation mit einer Gruppe verstärken kann, wenn die Gruppenidentität stark und die persönliche Identität weniger ausgeprägt ist. Gleichzeitig wird betont, dass die Auswirkungen der Anonymität auf Gruppenverhalten von vielen Faktoren, einschließlich der spezifischen Gruppenziele und -normen, abhängen.
AST
Die Adaptive Strukturierungstheorie (AST) untersucht, wie Gruppen und Individuen Technologien anpassen und nutzen, um mit Anonymität umzugehen. Sie betont, dass sich die Nutzung von Technologie im Laufe der Zeit entwickelt und verändert. Während AST die Flexibilität und Anpassungsfähigkeit von Technologienutzung in sozialen Kontexten betont, zeigt sie auch, dass die Anwendung und Wirkung von Anonymität durch die Interaktion von Technologie und sozialer Struktur beeinflusst wird.

Zusammenfassung der Theorien

Ziehe die Wörter in die richtigen Felder!

Die _____ untersucht die Anpassung der Technologienutzung in sozialen Kontexten. Anonymität kann Hierarchien in der computervermittelten Kommunikation durch das Filtern sozialer und physischer Hinweise verringern, was die _____ hervorhebt. Die _____ betont die Verstärkung der Gruppenidentität durch Anonymität. Die _____ thematisiert die Reduzierung der Selbstwahrnehmung und die mögliche Zunahme impulsiven Verhaltens, wobei diese Theorie in der Forschung umstritten ist.

Überprüfen

Deindividuationstheorie
Adaptive Strukturierungstheorie
SIDE-Theorie
Equalization Hypothesis

Fazit

Die Anonymität im Internet hat facettenreiche Auswirkungen auf die Kommunikation und soziale Interaktionen. Sie kann sowohl positive Aspekte wie Freiheit der Meinungsäußerung und Verringerung von Hierarchien, als auch negative Auswirkungen wie impulsives Verhalten und Gruppenpolarisierung mit sich bringen. Theorien wie die Deindividuationstheorie, die Equalization Hypothesis, die SIDE-Theorie und die Adaptive Strukturierungstheorie bieten tiefe Einblicke, zeigen jedoch auch die Komplexität und die kontextabhängigen Effekte der Anonymität. Dies unterstreicht die Notwendigkeit eines ausgeglichenen Verständnisses und verantwortungsvollen Umgangs mit Anonymität im digitalen Zeitalter.

Überprüfe dein Wissen

Überprüfe dein Wissen über die sozialen Aspekten von Anonymität im Web und wähle jeweils die korrekte Aussage:

✓ Fortschritt: 0/5

Anonymität führt generell zu einer schwächeren Gruppenbindung und weniger Polarisierung.

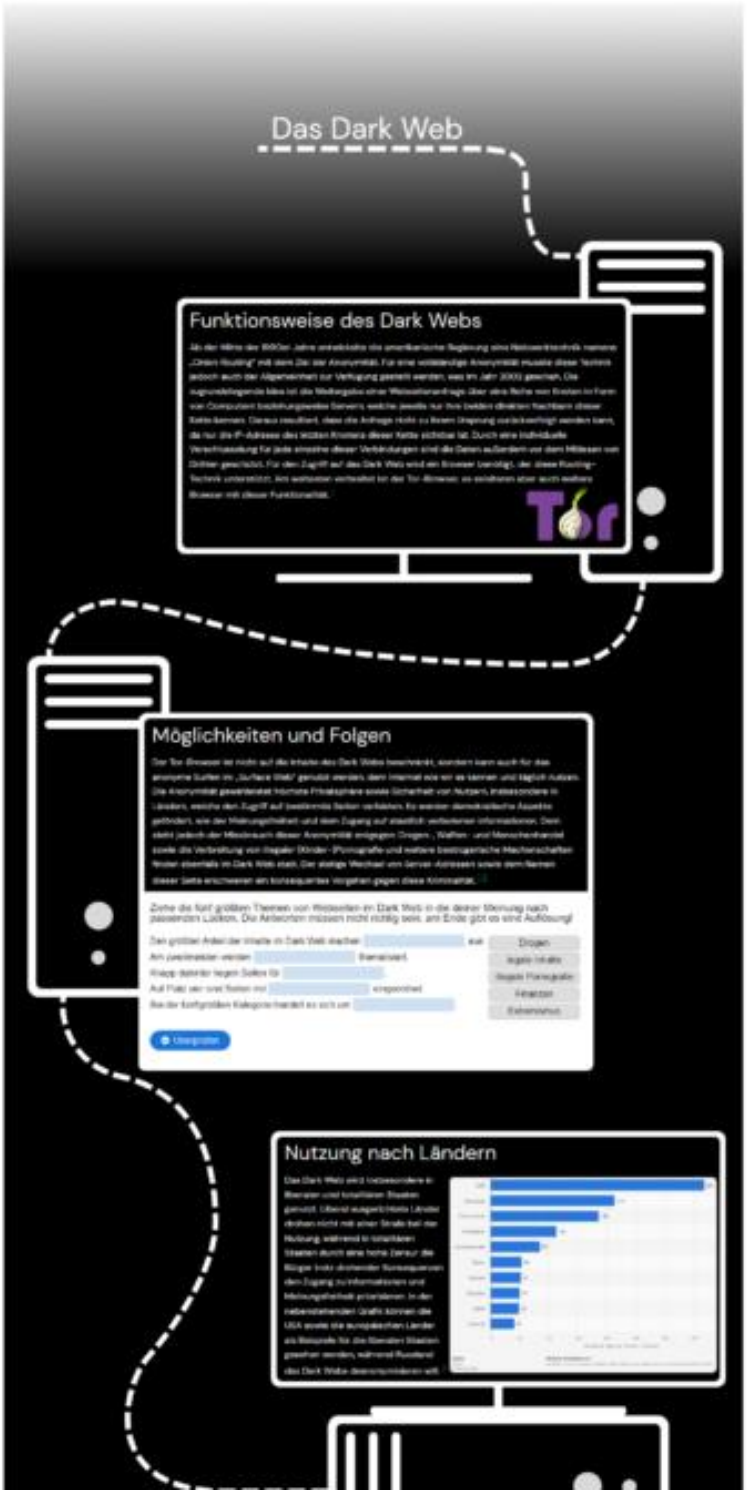
Anonymität in Online-Gruppen kann zu stärkerer Gruppenkohäsion und Polarisierung führen.

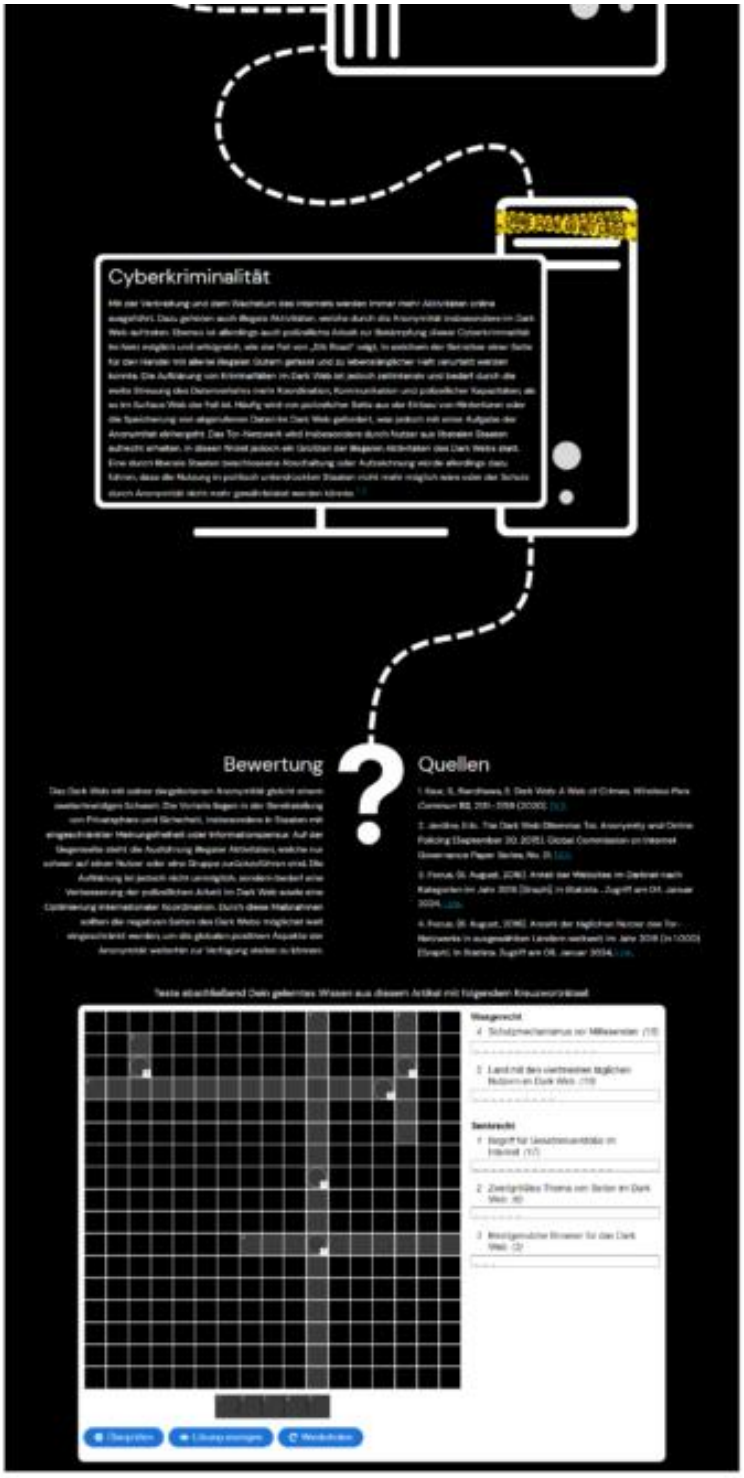
Literatur

CHRISTOPHERSON, Kimberly M., 2007. The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog". *Computers in Human Behavior* [online], 1 November 2007. Bd. 23, Nr. 6, S. 3038–3056. DOI 10.1016/j.chb.2006.09.001. Verfügbar unter: https://doi.org/10.1016/j.chb.2006.09.001

ENGLEHARDT, Steven, Dillon REISMAN, Christian EUBANK, Peter D. ZIMMERMAN, Jonathan MAYER, Arvind NARAYANAN und Edward W. FELTEN, 2015. Cookies That Give You Away. *Proceedings of the 24th International Conference on World Wide Web* [online], 18 Mai 2015. DOI 10.1145/2736277.2741679. Verfügbar unter: https://doi.org/10.1145/2736277.2741679

Dark Web


Das Dark Web
Funktionsweise des Dark Webs
Tor
Möglichkeiten und Folgen
Drogen
Nutzung nach Ländern


Cyberkriminalität
Bewertung
Quellen