Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

LEITFADEN
zur digitalen Identität

Wie ich meine digitale Identität souverän gestalte und Missbrauch vorbeugen kann

Zielgruppe

Heike Beismann, Matthias Fischer (2023): Leitfaden zur digitalen Identität. Wie ich meine digitale Identität souverän gestalte und Missbrauch vorbeugen kann. Internet-dokument. Erstellt im Förderprojekt digiSEM im Rahmen des Wettbewerbes Curriculum 4.0 nrw. Online verfügbar unter: www.orca.nrw.

Dieser Leitfaden richtet sich in erster Linie an Studierende, die wissen wollen, wie sie ihre eigene digitale Identität souverän gestalten können. Aber er richtet sich auch an alle anderen, die schon immer wissen wollten, was eine digitale Identität beinhaltet und was man tun muss, um sie im eigenen Sinn zu gestalten und vor Missbrauch zu schützen. Wir sind fast alle täglich im Internet und in den sogenannten Social Media unterwegs. Wir nutzen diese digitale Welt, um etwas nachzuschlagen, uns mit Bekannten und Freunden zu treffen, potenziellen Arbeitgebern unsere Stärken zu präsentieren und vieles mehr. Wir werden aber auch von diesen Medien benutzt. Unsere Daten, die wir eingeben, sind ein wertvolles Gut und wir sollten sie nicht leichtfertig mit anderen teilen oder aus der Hand geben. All das wissen wir theoretisch, dennoch verhalten wir uns oft nicht so, wie es angemessen wäre. Aus Bequemlichkeit, aus Unwissenheit oder weil uns die Konsequenzen nicht wirklich klar oder zu abstrakt sind. Dieser Leitfaden soll daher zunächst einmal sensibilisieren, für die Gefahren, aber auch vor allem für die Möglichkeiten, die sich bei der Selbstpräsentation im World Wide Web ergeben können. Gegenstand des Leitfadens ist damit die bewusste Gestaltung der eigenen digitalen Identität. Themen, wie z. B. sichere Authentifizierung im Internet, werden nicht betrachtet.

Wir möchten euch daher einladen herauszufinden, wie ihr euch im Internet geeignet präsentieren, eine eigene digitale Identität kreieren und diese kontrollieren könnt. Dazu findet ihr im ersten Teil dieses Leitfadens Hintergrundinformationen zur digitalen Identität und im zweiten Teil geben wir euch Handlungsempfehlungen zur vorteilhaften Online-Selbstdarstellung.

Bewusstsein für die eigene digitale Identität

Unsere Definition von digitaler Identität

Die digitale Identität ist das Bild einer Person, das sich aus der Gesamtheit aller Informationen über diese Person, die im Internet frei zugänglich sind, zusammensetzt.

Die genannten Informationen können Stammdaten von Benutzer-Accounts, Forenbeiträge, Blogbeiträge, Kommentare, Bilder, Standortdaten, Sprache (Spracherkennung) oder aber auch das Verhalten auf Webseiten und in Apps umfassen. Die Informationen können von Dritten oder von der betreffenden Person selbst willentlich oder unwillentlich in das Netz gespeist werden. Dritte können Familie, Freunde oder Bekannte sein aber auch Firmen, die mit diesen Informationen Geld verdienen bzw. andere fremde Personen oder Vereine, Gesellschaften, Arbeitgeber.

Darüber hinaus gibt es weitere isolierte digitale Identitäten einer Person, die z. B. durch Streaming-Anbieter oder andere Dienstleister im Internet durch gesammelte und algorithmisch ausgewertete Daten erstellt werden.

Digitale Identität in der wissenschaftlichen Literatur

Auch wenn der Begriff „digitale Identität“ bereits früher in der Literatur verwendet wurde, erfolgten explizite Definitionen erst in den Nullerjahren durch Expert:innen im Bereich Datenschutz und digitale Sicherheit.

Anlass für diese Begriffsbestimmungen war unter anderem die Entwicklung von Identitätsmanagementsystemen, welche z. B. im Bereich des E-Commerce, Kunden für Firmen authentifizierbar machen und gleichzeitig die Privatsphäre dieser Kunden wahren sollten.

Über diese technische Betrachtungsweise hinaus, wurden im EU-Projekt **FIDIS*** verschiedene Vorschläge erarbeitet, wie das komplexe Konzept Identität erweitert werden kann, um Aspekte der Online-Welt, wie Pseudonyme, Avatare aber auch maschinelles Profiling zu berücksichtigen.

Dazu zählte z. B. die Erweiterung bekannter soziologischer Identitätsbegriffe des „I“ und „Me“ sowie der „Idem- und Ipse-Identität“ oder die Idee der Einführung virtueller Personen. Eine tiefgehende soziologische Betrachtung der digitalen Identität übersteigt jedoch den Rahmen dieses Leitfadens.

Inzwischen gibt es Normen für Identitätsmanagement, in denen der Begriff Identität für diesen Kontext definiert wird. So definiert die DIN 24760 Identität bzw. partielle Identität als „Menge von Attributen [Merkmale oder Eigenschaften], die sich auf eine Entität [Dinge/Wesen, die erkennbar eine eigene Existenz haben] beziehen“. Generell können Entitäten (z. B. Menschen) mehrere (partielle) Identitäten aufweisen oder mehrere Entitäten sich eine (partielle) Identität teilen. In der Norm wird der Begriff „digitale Identität“ nicht definiert, im Identitätsmanagement ist aber davon auszugehen, dass die „Menge von Attributen, die sich auf eine Entität beziehen“ generell digital repräsentiert wird (Abbildung 1).

*Future of Identity in the Information Society

Die ITU (Internationale Fernmeldeunion) unterscheidet in ihrer Empfehlung zwischen einer holistischen Identität, die aus allen möglichen Informationselementen (Attributen), die einer Entität zugewiesen werden kann, besteht und den Identitäten welche Untermengen von Attributen der **holistischen*** umfassen (siehe Abbildung 1). Der Rahmen, d. h. Art und Umfang der Attribute wird vom jeweiligen Identitätsmanagement vorgegeben. Der Begriff „digitale Identität" wird hier als digitale Repräsentation der Informationen (Attribute) einer Entität definiert.

* holistisch = ganzheitlich

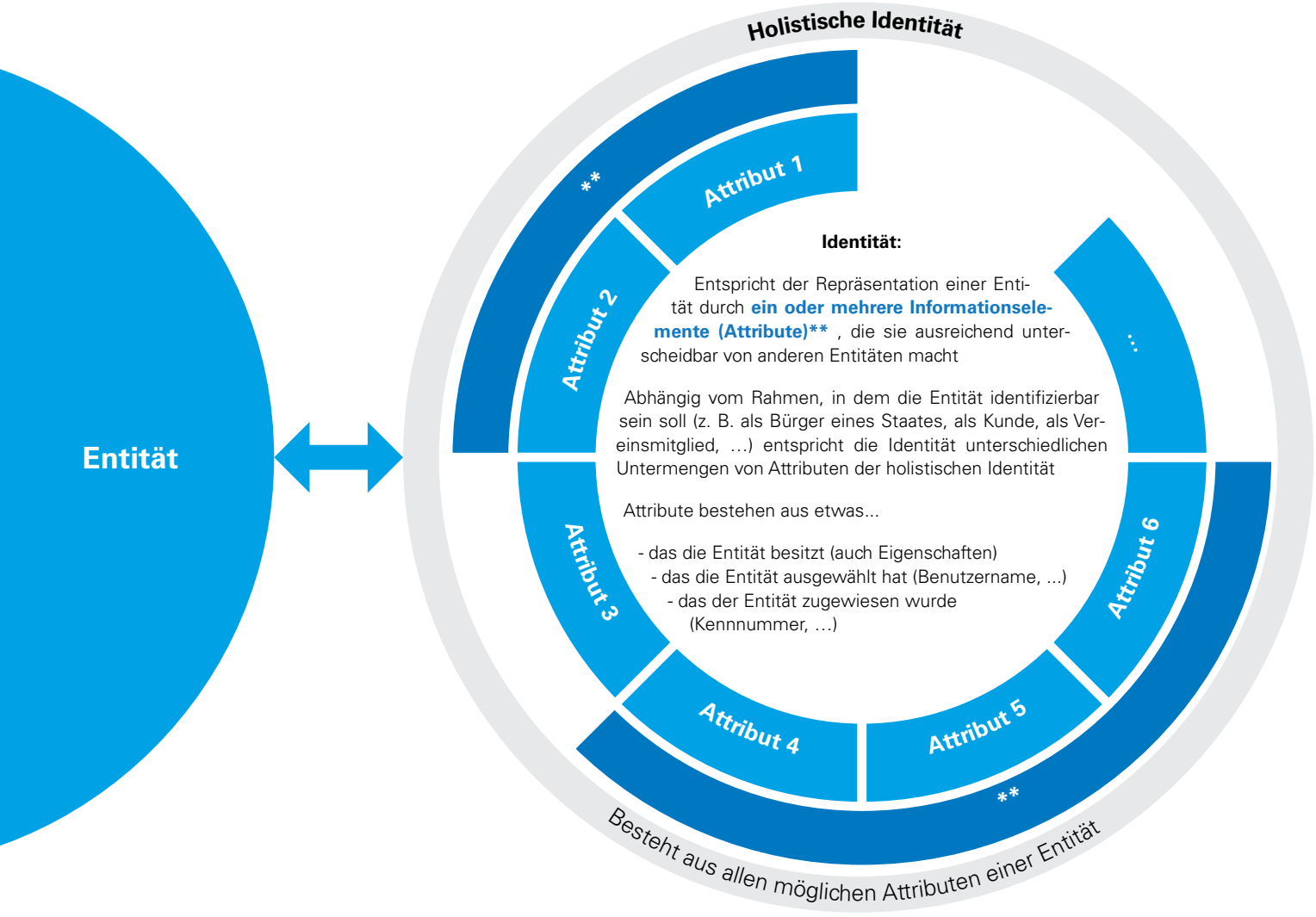


Abbildung 1: Identität und holistische Identität (verändert nach ITU-T Recommendation X.1252)

Die von uns definierte digitale Identität entspricht damit einer holistischen digitalen Identität, die wiederum einer vereinigten Menge aller digitalen Informationselemente, die einer Entität zugewiesen werden können, entspricht. Partielle digitale Identitäten werden dabei zugewiesen (Account-Management), abgeleitet (Profiling) oder selbst gewählt (Management eigener Identitäten).

Identitätsmanagement bietet i.d.R. ein Rahmenwerk, damit sich ein Subjekt in Kontakt mit Behörden, einem Dienstleistungsanbieter, usw. sicher authentisieren kann bzw. damit ein Subjekt sicher authentifiziert werden kann. Auf diesen engeren Sinn des Identitätsmanagements beziehen sich die „Digital Identity Guidelines" des **NIST***, nach denen nur ein Subjekt eine Identität besitzen kann.

*National Institute of Standards and Technology, USA

In diesem Zusammenhang wird die digitale Identität als Quelle von Daten (Attributen) für die Authentifizierung verstanden. Aus dieser Sichtweise heraus werden auch die avisierten digitalen Nachfolger der ID-Karten (z. B. dem Personalausweis) von der EU-Kommission sowie der Bundesregierung „Digitale Identitäten" genannt. Dabei handelt es sich, nach unserer Betrachtung, um partielle digitale Identitäten.

Neben den Merkmalen, die zur Authentifizierung dienen, werden einer digitalen Identität häufig noch weitere Attribute zugeordnet. Zum Beispiel im E-Commerce werden partielle Identitäten einer Entität einander zugeordnet (Identity Resolution) und so möglichst viele Informationen über eine Person zusammengeführt. Das betrifft sowohl verschiedene Datensätze zu einer Person innerhalb eines Unternehmens als auch firmenexterne Datenquellen. Das Ziel ist eine „360°-Identität" oder auch „Golden Profile" genannt, welche die Stammdaten (Namen, Adressdaten, …) ebenso umfasst, wie Informationen zum Sozialverhalten, den Aufenthaltsorten und den Vorlieben einer Person (Abbildung 2).

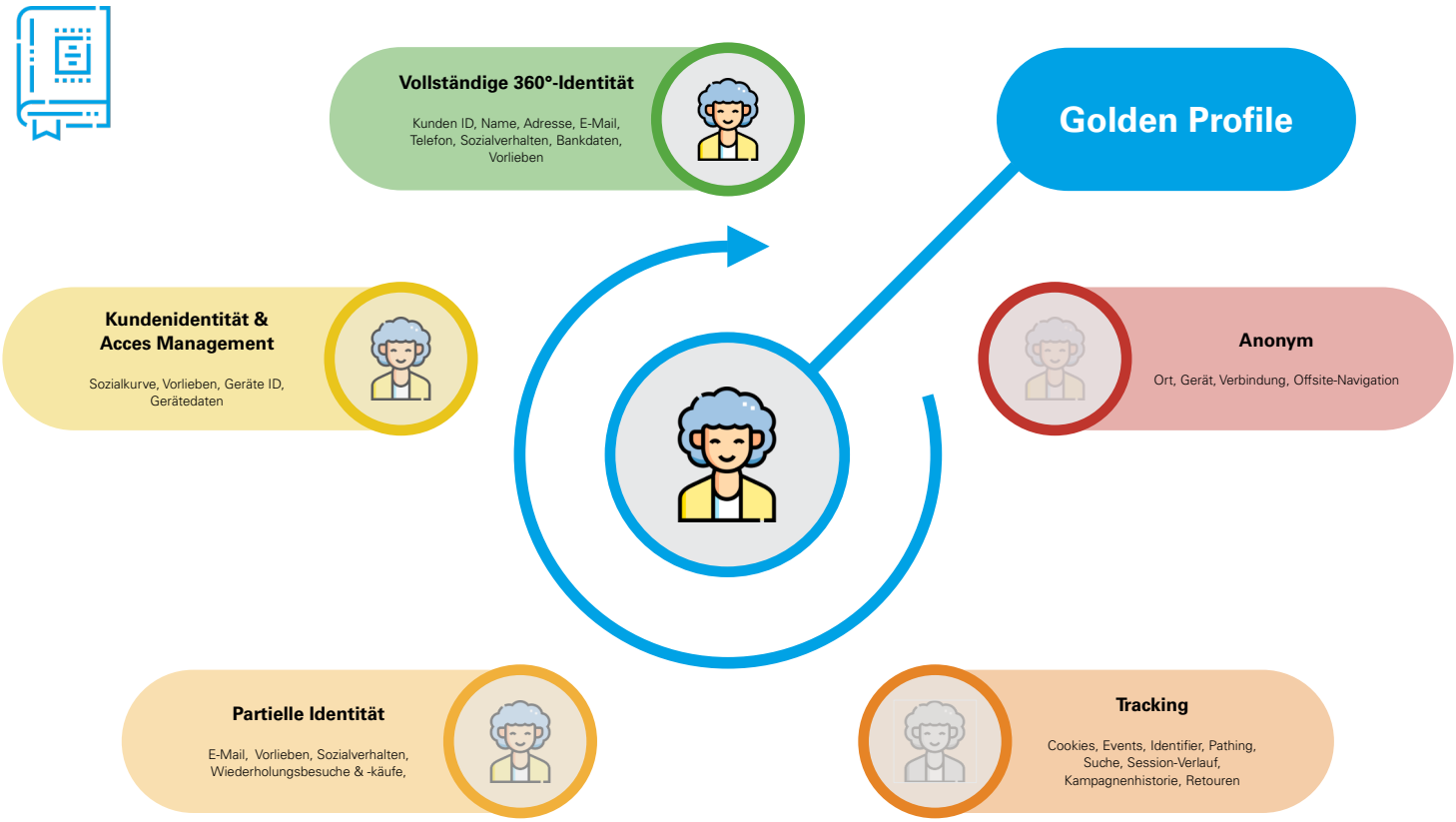


Abbildung 2: Erstellung einer 360°-Identität bzw. eines "Golden Profiles" (verändert nach Braun et al. 2022) ◈

Erstellt werden diese 360°-Identitäten über Profiling-Methoden, bei denen z. B. mit Machine-Learning Verfahren zueinander passende (also zu einer Person gehörende) partielle Identitäten gefunden werden. Die 360°-Identität kann dann zur Erstellung eines digitalen Zwillings eines Kunden herangezogen werden, welcher helfen soll, besser an den Kunden angepasste Produkte und Dienstleistungen anzubieten (Abbildung 2).

Wie in diesem Leitfaden später noch gezeigt wird, zählen insbesondere auch öffentliche Einträge bei Social Media Plattformen, aber auch Mitgliedschaften in Vereinen, in Parteien sowie alle anderen öffentlich zugänglichen Daten, die mit einer Person in Verbindung gebracht werden können, zu Attributen der digitalen Identität.

Aus diesen personenbezogenen Daten ergibt sich z. B. für Personalabteilungen, die Bewerber:innen überprüfen (Cybervetting, s. u.) ein Bild einer Person. Natürlich können auch potenzielle Freunde oder Partner auf diese Weise einen Eindruck von einem Menschen erhalten. In noch stärker systematischer Weise werden solche Daten beim Profiling (s. u.), z. B. durch potenzielle Arbeitgeber, zusammengetragen. Es ist vorstellbar, dass auch Banken bei der Vergabe von Krediten oder Versicherungen bei der Vertragsvergabe auf Profiling-Daten zurückgreifen.

Unsere digitale Identität hat damit einen großen Einfluss auf unseren beruflichen, finanziellen und privaten Erfolg.

Wen erreiche ich mit meinen Postings?

Wer mit Social Media Postings erreicht wird, hängt von verschiedenen Faktoren ab, wie z.B. der Plattform, die verwendet wird, der Zielgruppe, die angesprochen werden soll, und der Art des Inhalts, der geteilt wird. Im Allgemeinen werden die Menschen, die dem eigenen Profil folgen oder denen man selbst folgt, sowie deren Freunde und Bekannte erreicht.

Grundsätzlich gibt es zwei verschiedene Einstellungen zur Sichtbarkeit eines Social Media Kontos. Wenn das Konto öffentlich ist, kann jeder das Profil und die Beiträge sehen, der im Internet die Social Media Plattform und den Benutzernamen des Kontos aufruft. Zusätzlich kann ein einzelner Beitrag durch eine Suchmaschine von jedem Internetnutzer gefunden und angesehen werden. Wenn das Konto auf privat gesetzt ist, können eingeloggte Nutzer, die bestätigte Abonnenten dieses Kontos sind, das Profil und die Beiträge sehen.

Die durchschnittliche Reichweite von Facebook-Postings liegt bei rund 0,05% der Abonnenten dieser Facebookseite. Dies bedeutet, dass von 1.000 Abonnenten etwa fünf Personen auf einen Beitrag reagieren, diesen kommentieren oder teilen werden. Etwa 44,3 % der Social Media Nutzer folgen Profilen von Familie, Freund:innen und Bekannten. Damit werden die eigenen Beiträge dieser Nutzer wahrscheinlich auch am meisten von Familie, Freunden und Bekannten gesehen.

Es ist wichtig zu beachten, dass die Reichweite und die Interaktion mit den eigenen Beiträgen von der Art des Inhalts, dem Timing und der Art und Weise, wie die Beiträge präsentiert werden abhängen. Ein gut durchdachter und ansprechender Inhalt, der auf die Zielgruppe abgestimmt ist und zu einer geeigneten Zeit veröffentlicht wird, hat eine höhere Chance, gesehen und geteilt zu werden.

Grundsätzlich gilt, dass ein Social Media Beitrag dann erfolgreich ist, wenn die Zielgruppe ihn wahrnimmt. Damit ein Beitrag erfolgreich wird, gibt es einige Regeln, die für alle Plattformen berücksichtigt werden können. Das Wichtigste ist der Inhalt, dieser sollte relevant, informativ, unterhaltsam und hochwertig sein. Auch sehr wichtig ist der richtige Zeitpunkt zum Posten eines Beitrags. Zusätzlich sind hochwertige Bilder und Videos, die Aufmerksamkeit erregen und ansprechend sind, und passende Hashtags, die beitragsrelevant und kategorisierend sind, wichtig.

Auch hängt die Reichweite eines Beitrags von dem jeweiligen Algorithmus der Plattform ab.

Diese Algorithmen sind eine Reihe von Regeln, die Inhalte auf der jeweiligen Plattform einstufen.

Ihr entscheidet, welche Beiträge in welcher Reihenfolge angezeigt werden. Dabei gibt es drei Ranking-Faktoren, die die Algorithmen besonders beachten. Zunächst ist die Beziehung zwischen dem Autor des Inhalts und dem Betrachter wichtig. Wenn in der Vergangenheit wiederholt mit einem bestimmten Benutzer interagiert (Abonnement, Nachrichten, Kommentare) wurde, werden mit größerer Wahrscheinlichkeit die neuen Inhalte, die er veröffentlicht, angezeigt. Zudem ist das Interesse eines Benutzers von Bedeutung. Wenn der Algorithmus erkennt, dass ein Benutzer einen bestimmten Inhaltstyp oder ein bestimmtes Format mag, liefert er ihm mehr davon. Als drittes ist die Relevanz zu beachten. Aktuelle Beiträge oder Beiträge zu einem Trendthema werden häufiger angezeigt. Weitere Ranking-Faktoren sind die Häufigkeit der Nutzung der Plattform, die Anzahl der Abonnenten und gefolgten Profilen, sowie die Dauer eines Plattformbesuchs.

Auf den verschiedenen Plattformen sind verschiedene Zielgruppen aktiv. Wie viele Nutzer einen Post sehen hängt demnach auch von der Wahl der Plattform ab (Tabelle 1).

Tabelle 1: Übersicht über die verschiedenen Social Media Plattformen und deren jeweiligen Eigenschaften (verändert nach IHK München und Oberbayern 2022)

	Facebook	Instagram	Twitter	Pinterest	YouTube	LinkedIn/ Xing
Beschreibung	größter Kanal weltweit und in DACH-Region	Bildnetzwerk, mehr als 16 Millionen Nutzer in D	Plattform für Kurznachrichten	Bildnetzwerk, 3 Millionen Nutzer in D	weltweit größte Videoplattform, 77% aller deutschen Internetnutzer besuchen das Portal mindestens einmal im Monat	Karrierenetzwerke, LinkedIn international, XING DACH-Region
Stil der Inhalte	von seriös bis lustig	hochwertig, geschmackvoll	News	hochwertig, geschmackvoll	abwechslungsreich	seriös
Werbe-möglichkeiten	vielfältig	vielfältig	begrenzt	vielfältig	vielfältig	begrenzt
Zielgruppen	alle Altersgruppen, zunehmend viele Ältere, Kritische	ca. 18 bis 35 Jahre, mehr Frauen, technikaffin und offen	gemischt, etwa 18 bis 50 Jahre	gemischt, eher Frauen zwischen 18 und 50 Jahren	gemischt, eher zwischen 18 und 35 Jahre alt	gemischt, besonders ab 30 Jahre
Erreichbare Ziele	Image, Kundennähe, Traffic, Bekanntheit	Bekanntheit, Image	Kundennähe, Bekanntheit, Traffic, Image	Image, Traffic	Bekanntheit, Traffic, Image	Networking, Personalbeschaffung
Art des Contents	Text, Links, Bilder, Videos	Fotos & Videos mit Hashtags, Carousel-Ads möglich	Text, Bilder und Videos mit Links und Hashtags	Fotos mit Links	Videos mit Links	Text und Links
Zeitaufwand	mittel	mittel	hoch (viele Mitteilungen nötig)	mittel	hoch (erstellung der Videos)	gering

Generell werden in Deutschland mit Social Media hauptsächlich Leute unter 30 Jahren erreicht.

Bei den 14- bis 29-Jährigen sind es 88 Prozent, die wöchentlich oder häufiger Social Media nutzen. Ihr meistgenutztes Netzwerk ist Instagram.

In der Gesamtbevölkerung wird Facebook am häufigsten genutzt.

86,5 % der Gesamtbevölkerung in Deutschland sind auf Social Media vertreten. Bei den Nutzern ab 13 Jahren liegt dieser Anteil bei 98,7 %. Dabei besitzen die Nutzerinnen und Nutzer durchschnittlich 5,3 Accounts und verbringen im Schnitt 1 Stunde und 29 Minuten täglich in den sozialen Netzwerken. Zwar sind WhatsApp (83 % der Internetnutzer) und Facebook (60,7 %) immer noch die am meisten genutzten sozialen Netzwerke, liegen aber mit ihren 11,4 bzw. 11,0 Stunden Nutzungszeit pro Monat weit hinter TikTok mit 23,6 Stunden.

Obwohl die Zeiten der verschiedenen Social Media Plattformen variieren, scheint der Nachmittag im Allgemeinen eine beliebte Zeit zum Posten zu sein. Inhalte, die dienstags, mittwochs und donnerstags veröffentlicht werden, erhalten zudem mehr Aufmerksamkeit als Content, der an anderen Wochentagen geteilt wird (Abbildung 3).

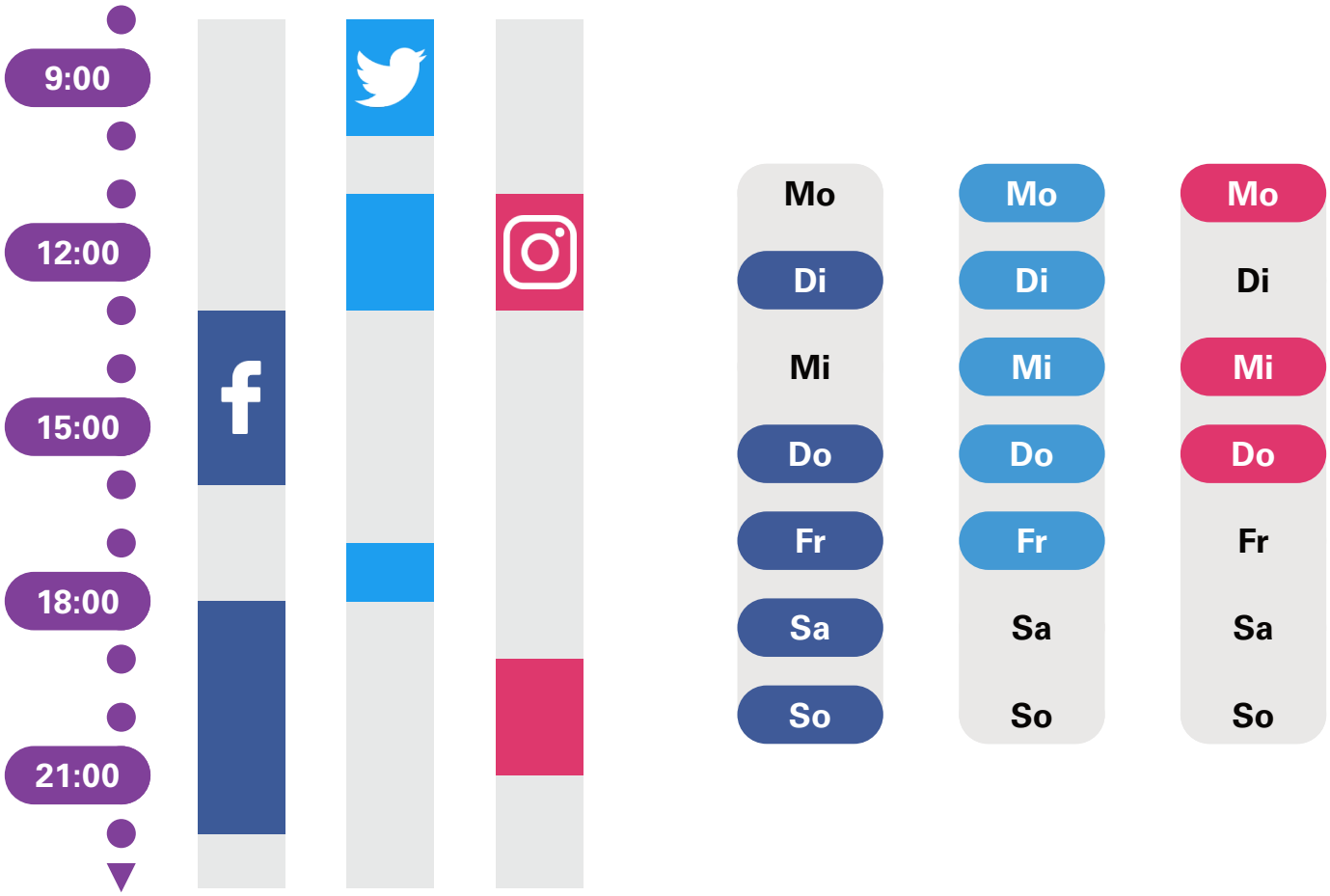
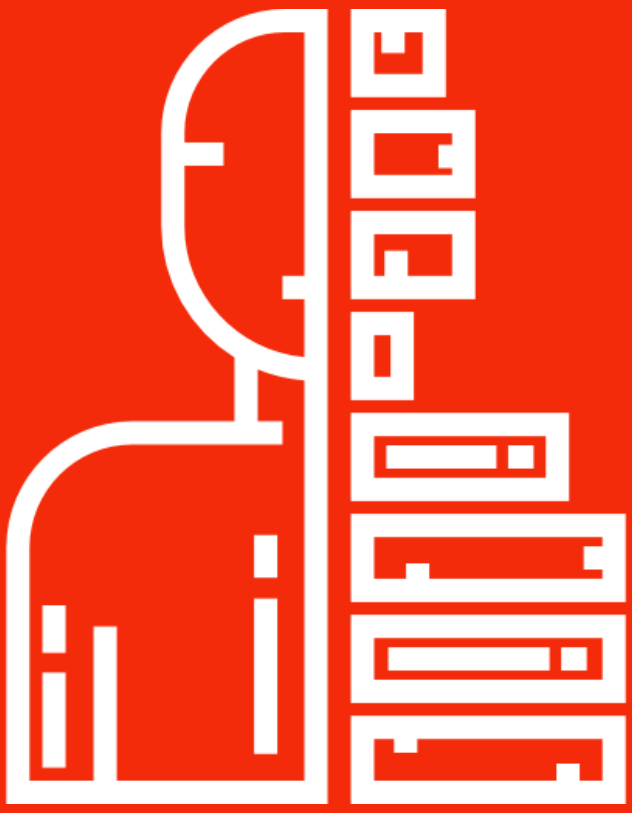


Abbildung 3: Übersicht über die besten Zeiten zum Posten bei Facebook, Twitter und Instagram (verändert nach Tamblé 2022) ◈

Welcher Beitrag an welchem Tag zu welchem Zeitpunkt gesehen wurde, kann in den Einstellungen des Profils gesehen werden. Bei Twitter kann bei „Twitter Analytics“ nach den „Top Tweets“ sortiert werden. Auf Facebook wird unter „Insights“ angezeigt, an welchen Wochentagen die meisten Likes erreicht wurden. Bei Instagram werden diese Informationen mit einem Geschäftsprofil in der Analysefunktion angezeigt

Wofür werden meine persönlichen Daten verwendet?



Wer besitzt und verarbeitet digitale Identitäten von mir?

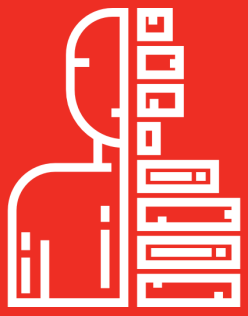
Die Nutzung von Internetdienstleistungen erfolgt in vielen Fällen unter Inkaufnahme einer damit verknüpften Datensammlung, welche z. B. für die Personalisierung von Werbung verwendet werden kann. So können Firmen wie Google und Amazon eigene Tracker (z. B. DoubleClick, Google Analytics, Amazon Technologies) zur Sammlung von aktuellen Informationen über die Nutzer verwenden.

Neben Website-eigenen Trackern werden **3rd Party Cookies*** von sog. **Data Brokern**** für die Datensammlung verwendet.

* Cookies dritter Parteien

** Unter Data Brokern werden Firmen verstanden, welche in der Sammlung von Daten und dem anschließenden Verkauf spezialisiert sind.

Die bekanntesten Data Broker sind Axicom, Experian, Rapleaf und Datalogix.



Weiterhin werden Apps, wie z.B. Facebook und Instagram von Meta (ehemalig Facebook), zur Datensammlung verwendet. Bei der Facebook App werden bis zu 79,5 % und bei der Instagram App 69,2 % der persönlichen Daten gesammelt. Unter persönliche Daten fallen unter anderem Informationen wie Namen, Geburtstag, E-Mail, Größe, Gewicht, Bankinformationen, sowie Angaben auf anderen sozialen Netzwerken, welche mit der App verlinkt sind. Die gesammelten Daten werden einer Identität zugewiesen, welche von Data Brokern unterschiedlich kategorisiert werden kann. Beispielhafte Identitätskategorien amerikanischer Data Broker sind **Urban-Scramble*** und **Rural Everlasting****. Die Überkategorien werden weiter in Kategorien, wie „erwartende Eltern“ oder „auf Cholesterin fokussiert“ unterteilt. Somit können Werbeagenturen ihre angezeigte Werbung im Internet an die vermuteten Interessen des Benutzers anpassen.

* große Population mit niedrigem Einkommen

** alleinstehende Menschen über 66 mit geringem Bildungsstand und geringem Eigenkapital

Hierbei ist zu beachten, dass Data Broker sich in einer sog. **Co-Opetition*** befinden.

*** Zusammengesetzt aus den englischen Wörtern für Kooperation (cooperation) und Wettkampf (competition)

Co-Opetition beschreibt die situationsbedingte Zusammenarbeit oder Konkurrenz von Data Brokern, abhängig von der Komplementarität und den Zusammenführungskosten von Datensätzen verschiedener Firmen.

Werden verschiedene Daten miteinander kombiniert, kann der finanzielle Wert der Kombination für einen Data Broker größer sein als die Summe der Einzelwerte der Daten. In diesem Fall verhalten sich die Daten „super-additiv“. Es gibt jedoch auch Datenkombinationen, deren Wert geringer ist als die Summe der Werte der Einzeldaten (sub-additive Daten). Diese Dateneigenschaften bilden die Basis der Zusammenarbeit und der Konkurrenz zwischen verschiedenen Data Brokern bzgl. des Datenaustauschs.

Datensammlung: Technische Hintergründe

Das Hypertext Transfer Protocol (HTTP) bildet die Basis der Datenkommunikation im World Wide Web. Hierbei findet die Kommunikation zwischen dem Webbrowser (auch client oder user agent genannt) und dem Webserver statt. Im Webbrowser werden die Informationen aus dem Uniform Resource Locater (URL) für die Verbindung zum Webserver gelesen und für den Aufbau einer Verbindung zum Webserver inklusive Anfrage genutzt. Auf diese Anfrage „antwortet" der Server und die Verbindung wird beendet. Dieses Grundgerüst wird als zustandslos bezeichnet, d.h. der Webserver antwortet auf eine neue Anfrage, ohne Erinnerungen (Speicher) an die vorherige Anfrage.

Cookies beinhalten u. a. Informationen über den Ursprungsserver und darüber, wie sie zu lesen sind. Hiermit kann ein Web-Server einen Zustand (State) aufrechterhalten und eine Erinnerung (Memory) an vorherige Anfragen besitzen. Die Informationen innerhalb der Erinnerung werden mit den Informationen aus dem neuesten gesendeten Cookie verglichen und aktualisiert.

Durch die Aufrechterhaltung eines Zustandes über Cookies können Komfortfunktionen, wie z. B. Shoppingfunktionen (der Warenkorb bleibt auch nach dem Verlassen der Webseite bestehen und wird erst durch das manuelle Entfernen von Waren oder dem Kaufabschluss geleert) und vorgespeicherte Login-Information (z. B. die Anfrage vom Browser, ob das Passwort gespeichert werden soll, gefolgt von der automatischen Ausfüllung der Login-Information bei der nächsten Anmeldung) geschaffen werden.

Ein Cookie ist ein minimaler Datensatz an Information in Form eines Strings (einer endlichen Folge von Zeichen, z. B. Buchstaben, Zahlen oder Wörtern) welcher zwischen dem Webbrowser und dem Webserver übermittelt wird (Tabelle 2).

Tabelle 2: Übersicht der Attribute und zugehörigen Definitionen eines einfachen Cookies bzgl. Ursprung, hinterlegte Information und Randbedingungen des Transfers (verändert nach Cahn et al. 2016) ◈

Cookie-Attribut	Definition
Name	Identifikationsmerkmal eines Cookies bzgl. eines bestimmten Servers
Value	Beschreibt die Information, welche im Cookie hinterlegt ist. Informationen können verschlüsselt werden
Host	Beschreibt den Ursprungsserver des Cookies. Hierdurch wird zwischen Cookies von ersten (1st party) oder dritten (3rd party) Parteien unterschieden
Path	Setzt Randbedingungen für den Zeitpunkt, wann der Server den Cookie zurück sendet
Expires	Beschreibt die Dauer der Gültigkeit eines Cookies. Hiermit wird zwischen sitzungsspezifischen und dauerhaften Cookies unterschieden
Secure	Hiermit wird die sichere Transferart mittels SSL (Secure Socket Layer) oder HTTPS festgelegt
HTTPOnly	Spezifiziert ob Programme bei der Seite des Nutzers (Client) auf de Cookie zugreifen können
IsDomain	Spezifiziert, ob ein Cookie zum Host oder zu einem zugehörigen Teilbereich gesendet werden soll. Das IsDomain-Attribut ist ein Teil des Host-Attributs und spezifisch für Firefox

Grundsätzlich werden Cookies nach der Art der Speicherung in sitzungsspezifische (session), dauerhafte (persistent) oder Flash-Cookies eingeteilt sowie nach dem Host in Cookies von Erst- und Drittanbietern eingeteilt.

Cookies zweiter Parteien gibt es nicht, lediglich Datensätze zweiter Parteien, welche den Austausch von Daten zwischen Firmen beschreiben.

Sitzungsspezifische Cookies werden temporär im RAM gespeichert und werden nach dem Schließen des Browsers gelöscht. In dieser Art von Cookies werden sitzungsidentifizierende Informationen hinterlegt, ohne Zugriff auf den nicht-flüchtigen Speicher (z. B. eine Festplatte). Dauerhafte Cookies können als Gegensatz zu sitzungsspezifischen Cookies gesehen werden, da sie permanent auf dem nicht-flüchtigen Speicher hinterlegt und bei dem Schließen des Browsers nicht gelöscht werden. Sie beinhalten einen Überblick über die websitespezifischen angegebenen Präferenzen eines Benutzers und zählen die Anzahl von besuchten Webseiten. Flash Cookies beinhalten kleine Flash Dateien, welche ähnliche Informationen besitzen wie die restlichen Cookies. Jedoch können Flash Cookies nicht direkt vom Browser gelöscht werden, sondern müssen manuell oder mit einem spezifischem Add-on (Browser-Erweiterung) gelöscht werden.

Cookies von ersten und dritten Parteien unterscheiden sich in der Anwendung und von wem sie ausgelegt werden.

Cookies erster Parteien werden grundsätzlich für die Leistung und Funktionalität der Webseite verwendet.

Hierbei sei darauf verwiesen, dass analytische Services, z. B. Tracker wie Google Analytics auch zum Bereich Leistung gezählt werden.

Unter Cookies von dritten Parteien werden Cookies zusammengefasst, welche vorwiegend für Personalisierung, Werbung und Datensammlung verwendet werden.

Grundlegend werden Cookies von dritten Parteien von Domänen platziert, welche außerhalb der in der URL angezeigten Domäne liegen.

Im Jahr 2016 wurden die verwendeten Cookies von den Top 100.000 Webseiten über ein Web Crawler System abgerufen, gesammelt und analysiert. Das System fragte Webseiten auf Basis vorgegebener Parameter ab, um die zugehörigen Cookies zu protokollieren und anschließend auszuwerten. Hierdurch wurde ein Anteil von 36,58 % Cookies von Erst- und 63,42 % Cookies von Drittanbietern, bei einer Gesamtanzahl von 1.895.023 Cookies bestimmt. Lediglich 0,24 % wurden mit dem Sicher-Attribut gesetzt, also lieferten 99,8 % der Cookies eine Angriffsmöglichkeit für Externe. Zusätzlich besaßen 80 % der gesammelten Cookies maximale Genehmigungen, was verschiedene Bedeutungen für Cookies von Erst- und Drittanbietern hat. Bei Cookies von Erstanbietern kann ein Angreifer Cookies mit maximaler Genehmigung nutzen, um z. B. Login-Daten abgreifen. Bei Cookies von Drittanbietern wird durch das Setzen von maximaler Genehmigung das Sammeln persönlicher Informationen erleichtert.

Basierend auf der Ankündigung des **third-party phase-out*** im Februar 2020, sowie einer folgenden Ankündigung von Google, Cookies von Drittanbietern bis zum Jahr 2022 eingestellt zu haben, ist fraglich ob die genannten Methoden der Sammlung von Benutzerinformationen weiterhin bestehen bleiben.

* Eine schrittweise Einstellung von Cookies von Drittanbietern

Zusätzlich ist unklar, ob hierdurch die Privatsphäre von Internetbenutzern langfristig verstärkt geschützt wird, oder welche neuen Techniken und Methoden zukünftig für das Sammeln von Benutzerinformationen verwendet werden und ob diese tiefer in die Privatsphäre eindringen als bisherige Methoden.

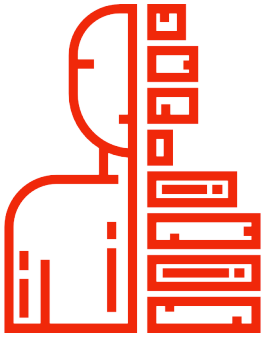
Die Datensammlung auf Websites erfolgt mithilfe eines Pixel-Tracking über sogenannte Page Tags.

Page Tags können als ein kleines Stück Programmiercode verstanden werden, welches nahezu unerkennbar auf Webseiten als ein 1 Pixel großes Bild hinterlegt werden kann. Über dieses Bild können, während der Benutzung einer Webseite, das Browsingverhalten (aufgerufene Unterseiten, Orte des schwebenden Mauszeigers, etc.), sowie jegliche Interaktionen des Nutzers mit der Seite protokolliert werden. Auf der Festplatte hinterlegte Daten sind dabei jedoch nicht sammelbar. Der Prozess der Datensammlung wird durch sog. Events auf der Webseite gestartet. Diese Events beinhalten z. B. das Klicken oder eine Tastatureingabe. Analog zum Page Tag erfolgt die Datensammlung über Apps mittels sog. Software Development Kits (SDK), welche in der für die App verwendete Programmiersprache, geschrieben wurden. Hierbei ist wichtig zu verstehen, dass der Rahmen der Datensammlung abhängig von den gewährten Rechten der App ist. Wurde z. B. die Erlaubnis für die Kamera gegeben, so können die Bilder ausgelesen und Informationen über das Umfeld, wie die Hausnummer, gesammelt werden. Grundlegend werden über E-Mails weniger Daten gesammelt. Dem zugrunde liegen die automatische Erkennung von schädlichen E-Mails und standardmäßige Blockierung von Page Tags durch E-Mail-Programme, z. B. Outlook. Das Datensammeln erfolgt hierbei über drei Mechanismen. Der erste Mechanismus erfolgt ähnlich wie bei den Webseiten, jedoch wird hier ein 1 Pixel großes Bild ohne Codeanteil verwendet. Dieses Bild kann nach dem Öffnen der E-Mail von einem Trackingserver abgerufen werden. Wodurch die IP-Adresse des Benutzers, der Öffnungszeitpunkt der E-Mail sowie Informationen zum Betriebssystem gesammelt werden können. Die zweite Methode überprüft die erfolgreiche (oder fehlgeschlagene) Zustellung der E-Mail an den Benutzer über Status-Meldungen (Delivery Status Notification) zwischen den Mail-Servern. Der dritte Mechanismus beinhaltet das Messen von Links, welche angeklickt werden. Hierfür müssen die Links über sog. Trackingserver führen oder über einen Kampagnen-Tracking-Code auf der Zielwebsite gemessen werden.

Auch über Werbung auf Webseiten werden Daten gesammelt, indem sog. Ad-Tags verwendet werden. Diese Ad-Tags erlauben das Hochladen von Werbung und das Messen der zugehörigen Impressionen (Anzahl, wie oft eine Werbung gesehen wird) und Klicks. Die Messung der Klicks kann dem Problem unterliegen, dass die **Webseiten zu schnell gewechselt werden***, sodass keine Messung durchgeführt werden kann.

* Aufbau der verlinkten Webseite erfolgt schneller als die Messung

Aus diesem Grund erfolgt oftmals eine Weiterleitung über spezielle Server, welche die Messung durchführen. Weiterhin kann eine sekundäre Messung über das Page Tag der Zielwebseite erfolgen. Insgesamt werden Klicks, Impressionen, Weiterleitungen und der Umsatz aus den Weiterleitungen gesammelt. Diese Daten werden jedoch nicht nur einmalig aufgenommen, sondern können in allen beteiligten Ad-Servern, Analyse-Systemen und Weiterleitungsservern hinterlegt sein. Dasselbe System der Datensammlung wird auch von Social-Media-Plattformen für die Werbung von Firmenkunden unter dem Begriff Paid Social verwendet. Hierbei wird jedoch ein spezifisches Ad-Tag verwendet, z. B. das Facebook-Tag, welches genau wie ein Ad-Tag funktioniert, jedoch auf Werbekanäle/-profile auf der eigenen Plattform verweist, somit wird die Webseite nicht gewechselt. Weitere verwendete Methoden werden Owned und Earned Social genannt. Owned Social umfasst dabei die gesammelten Daten von Kanälen/ Profilen, welche von dem Unternehmen auf einer Plattform, z. B. Facebook, selbst betrieben werden. Die Betreiber dieser Kanäle/ Profile, haben oftmals Zugriff auf eine von der Plattform gestellte Datensammlung.



Solche Sammlungen können statistische Auswertungen, z. B. den Zusammenhang zwischen der Zahl der Abonnenten und den Likes enthalten oder sog. **Application Programming Interfaces*** umfassen.

* Programmierschnittstellen für die Datensammlung

Sie erlauben jedoch keinen Zugriff auf spezifische Informationen über die Benutzer:innen, sondern lediglich Informationen zur Erfolgsbeurteilung des eigenen Kanals. Earned Social umfasst alle frei zugänglichen Informationen wie z.B. Posts und Tweets, welche auf eine Firma oder ein Branding verweisen. Diese Informationen können über Crawler (Definition siehe S. 25) gesammelt und in einer anschließenden Textanalyse ausgewertet werden. Hierdurch können z. B. Informationen über das Ansehen einer Firma in verschiedenen Altersklassen gewonnen werden. Es ist jedoch zu erwähnen, dass Menge und Personalisierbarkeit käuflich erwerbbarer Daten durch die Betreiber der Social Media-Plattformen, z. B. durch Aggregation, stark begrenzt werden. Personalisierbarkeit von Daten ist die Voraussetzung für sogenanntes „People-based Marketing", welches versucht, in einer automatisierten 1:1 Marketinganssprache, auf ein Individuum abgestimmte Angebote zu unterbreiten.

Werbefinanzierung im Internet

Grundlegend wird das Aufrufen einer Webseite aufgeteilt in den URL-Aufruf und die Weiterleitung der Browserinformationen an den mit der URL bezeichneten Server. Der Server verarbeitet nach vordefinierten Regeln die Anfrage des Browsers. Dieser Vorgang wird als Web Traffic bezeichnet, welcher die Grundlage für digitale Werbung bildet.

Werbeanbieter und Webseiteninhaber können verschiedene Methoden nutzen, um den Web Traffic zu den eigenen Webseiten und somit den Umsatz zu erhöhen, wie z. B. Suchmaschinenoptimierung (Search Engine Optimization - SEO).

Dies umfasst das inhaltliche Anpassen der eigenen Webseite, indem Schlüsselwörter hinzugefügt werden, welche von der Kundenzielgruppe, z. B. auf der Suche nach einem bestimmten Produkt, häufig in eine Suchmaschine eingegeben werden. Die Webseiten werden somit höher auf der Ergebnisliste der Suche angezeigt. Hierbei werden die angezeigten Ergebnisse in natürliche und bezahlte (sponsored) unterteilt. Natürliche Ergebnisse umfassen alle Ergebnisse, welche eine hohe Relevanz (gemessen an Artikellänge, Kompetenz des Autors, Übereinstimmung mit Titel, Schlüsselwörter, Links usw.) für die verwendeten Suchbegriffe besitzen. Es können auch Anzeigen als Suchergebnisse von Search Engines angezeigt werden, je nach Ort und Suchanfrage, welche von der betreffenden Seite bezahlt werden. Die Ergebnisliste wird von der Search Engine, nach der ermittelten Relevanz bezüglich der Suchbegriffe sortiert. Schlüsselwörter einer Website, welche für die Relevanz von großer Bedeutung sind, werden von den Webseiteninhabern in Abhängigkeit von der Zielgruppe und dem Webseiteninhalt selbst gewählt. Oftmals werden Methoden wie Text Spam, z. B. die Wiederholung von wenigen Schlüsselwörtern durch unsichtbaren Text oder die Erhöhung der Anzahl verschiedener Schlüsselwörter durch zusätzlichen Text, für eine künstliche Erhöhung der Relevanz in der Bewertung durch die Suchmaschine verwendet.

In beiden Beispielfällen nehmen menschliche Benutzer:innen die Webseite durch die Manipulationen nicht als relevanter war.

Aus dem erreichten Web Traffic können Webseiten mittels Werbung Gewinn machen, indem sie verschiedene Marketingstrategien wie Online Behavioral Advertising, Collaborative Environment und Real Time Bidding verwenden.

Durch Online Behavioral Advertising wird die angezeigte Werbung an die digitale Identität des Benutzers angepasst. Collaborative Environment beschreibt die Zusammenarbeit zwischen Unternehmen, Service-Anbietern und Werbefirmen zur Optimierung des Werbeaufwands und resultierendem Umsatz, durch eine kundenorientierte Werbegestaltung. Zur Anpassung der Werbung werden jedoch keine digitalen Identitäten verwendet, sondern Befragungen durchgeführt.

Real Time Bidding beschreibt in diesem Zusammenhang das Versteigern von Werbeplätzen auf Webseiten, während diese nach dem Aufrufen aufgebaut werden. Bei dieser Form der Werbeplatzversteigerung wird zunächst eine Anfrage an einen elektronischen Marktplatz gesendet, dem sogenannten Ad Exchange. Auf diesem können Firmen oder andere Plattformen nach festgelegten Parametern auf Gebote reagieren und bestimmte Werbeplätze ersteigern, welche zu Nutzer:innen einer bestimmten Zielgruppe gehören. Das Real Time Bidding dauert ca. 100 ms.

Die Effektivität und Erfolgsrate der Werbung können über verschiedene Metriken gemessen werden:

- Page Views: Beschreibt wie oft eine Webseite gesehen wird (gesehen heißt hierbei geladen bzw. aufgerufen; ein neues Laden der Webseite führt zu einem weiteren Page View).
- Bounce rate: Beschreibt den prozentualen Anteil der Nutzer:innen, welche ohne eine Interaktion die Webseite wieder verlassen haben.
- Ad Impressions: Beschreibt, wie oft Nutzer:innen Sichtkontakt mit einem Werbebanner beim Aufruf/Besuch der Webseite aufbauen und mit dieser interagieren.
- Ad-Clicks: Beschreibt das Anklicken der Werbung beim Besuch der Webseite.

Da beim Aufruf von Webseiten, nicht nur die gewünschte Webseite, sondern auch Werbung geladen wird, wird ein Teil der Bandbreite für nicht angefragten „Service“ verwendet. Hat der Benutzer ein limitiertes Datenvolumen, so lässt sich die für die Werbung benötigte Bandbreite in Kosten umrechnen und mit den Ausgabekosten des werbenden Unternehmens vergleichen. Zusätzlich dazu müssen privatsphärenspezifische Kosten bzgl. der digitalen Identität mit einbezogen werden.

„Kosten", die durch Werbung verursacht werden:

- 19% aller gesendeten Anfragen vom Browser beziehen sich auf Werbung und Analyse. Das entspricht ca. 8,2 % des Datenvolumens eines durchschnittlichen Handybenutzers.

- Bis zu 9% des Energieverbrauchs eines Mobiltelefons kann auf das Laden und Anzeigen von Werbung zurückgeführt werden.

- Die Daten von 97% aller Benutzer:innen werden gesammelt und mindestens einmal pro Jahr in einer digitalen Identität zusammengefasst.

- Bezogen auf das Datenvolumen bezahlen Benutzer:innen durchschnittlich das Dreifache an Kosten für Werbung als das werbende Unternehmen.

Weiterhin ist es kein Geheimnis, dass die Werbung als störend wahrgenommen wird und ein potenzielles Sicherheitsrisiko für die Benutzer bildet. Beispielsweise können Hacker Zugriff auf einzelne Werbeplätze erlangen, um Nutzer:innen auf dubiose Webseiten weiterzuleiten und von diesen zu profitieren.

Für die eigene Sicherheit, verbesserte Ladezeiten und Vermeidung von störender Werbung können Applikationen zum Blockieren von Werbung (Ad-Blocking) wie Brave, Ghostery und Adblock Plus verwendet werden.

Dies ist jedoch nicht im Sinne der Webseiteninhaber, weshalb verschiedene Ansätze gegen Adblocker angewendet werden. Manche Webseiten fordern das Abstellen von Adblockern beim Aufrufen der Webseite, ansonsten wird der Zugriff blockiert. Dies kann jedoch dazu führen, dass die Benutzer die Webseite verlassen oder frei zugängliche Alternativen verwenden. Andere Webseiten versuchen aufklärend dem Benutzer entgegenzukommen, indem sie über die Finanzierung der Webseite informieren und Abonnenten den Zugang gegen eine Gebühr anbieten. Schließlich gibt es Adblocker, wie Adblock Plus, die sich die Freischaltung der Werbung einer Firma von dieser bezahlen lassen (Werbung wird auch mit Adblocker angezeigt). Solche Maßnahmen wirken sich jedoch nur auf den einen Adblocker aus, durch andere Adblocker wird die Werbung weiter geblockt. Insgesamt führt das Adblocking zu einem Webtraffic-Verlust und somit zu einem Verlust der Werbemöglichkeiten und -finanzierung.

Durch Ad-Blocker besitzen Nutzer:innen die Möglichkeit zu bestimmen, welche Webseiten sie mit Werbeeinnahmen unterstützen möchten und welche nicht. Ein pauschales Blockieren von jeglicher Werbung durch einen großen Anteil an Nutzer:innen kann jedoch Webseiten die Finanzierung erschweren, wodurch Betreiber in Zukunft womöglich auf andere Modelle zur Geldbeschaffung zurückgreifen müssen.

Ein Beispiel für ein solches Modell ist die Werbe-**Opt-In***-Funktion des Brave Browsers. Hier ist Werbung standardmäßig deaktiviert. Man kann sich aktiv dafür entscheiden, Werbung zu aktivieren.

* Opt-In = sich aktiv für etwas entscheiden (von optieren = sich für etwas entscheiden)

Ein neues, bisher noch theoretisches Konzept ist ein sog. PIMS (Personal Information Management System). Hierbei werden persönliche Daten als Besitz der jeweiligen Person gesehen. Außerdem besitzt bei dieser Herangehensweise jede:r Nutzer:in die Möglichkeit selbst zu entscheiden, welche Informationen geteilt werden und welche nicht.

Cybervetting

Cybervetting ist der Prozess, bei dem eine Person Online-Informationen sammelt, um die Eignung einer anderen Person für eine bestimmte Aufgabe zu beurteilen.

Durch die regelmäßige Nutzung von sozialen Medien sowie Suchmaschinen, Suchaggregatoren und sich entwickelnden Internet- und Kommunikationstechnologien können Menschen auf mehr und andere Informationen über aktuelle und potentielle Arbeitnehmer zugreifen.

Eine solche Überprüfung wird oft als Internet-Überwachung, Social Media Background Check, Social Media Screening, Online-Screening oder Social Media Profiling bezeichnet - was die Rolle der sozialen Medien beim Cybervetting hervorhebt. Beim Cybervetting können nichtstaatliche, nicht-institutionelle Online-Werkzeuge oder -Seiten verwendet werden (z. B. Suchmaschinen und soziale Netzwerke), um informelle, oft persönliche Informationen über eine Person zu sammeln. Unternehmen nutzen diese Möglichkeit in den vergangen Jahren zunehmend, da die gefundenen Informationen im Vergleich zu konventionellen Einstellungsverfahren oft ein zusätzliches Bild einer Person transportieren. Cybervetting wird als Ergänzung oder Erweiterung von konventionellen Strategien gewertet. Nach einer Studie aus dem Jahr 2018 aus Amerika nutzen 70 Prozent der befragten Unternehmen Cybervetting, um Personen im Bewerbungsprozess zu überprüfen. Der Nutzen von Cybervetting kann in drei Bereiche unterteilt werden:

1. Überprüfung: Es werden Bewerber:innen aufgrund ihres digitalen Fußabdrucks bereits im Bewerbungsprozess aussortiert.
2. Effizienz: Der Prozess der Findung geeigneter Kandidat:innen kann beschleunigt werden.
3. Interaktionen: Es ist möglich, Prozesse, welche zuvor mit intensiver Interaktion einhergingen durch die Methode des Cybervettings zu ersetzen.

Aufgrund dieser Optimierung des Einstellungsprozesses ist Cybervetting für Arbeitgeber ein wertvolles Werkzeug, weshalb es bereits zum Alltag vieler Personaler:innen gehört. Das von vielen Firmen als Risikomanagement eingestufte Cybervetting dient der Suche nach sogenannten „Red Flags".

Red Flags sind ein Indikator dafür, ob eine Person als mögliches Risiko für die Firma oder als potentieller Arbeitnehmer gesehen wird.

Red Flags umfassen Anzeichen von fehlender Reife, Anzüglichkeit, Kriminalität oder Unehrlichkeit. Frei zugängliche Bilder, welche über Google oder Facebook gefunden werden können, sind Hauptbestandteil dieser Evaluierung. Einige Arbeitgeber geben sogar an, eingestelltes Personal zu cybervetten, um es auf ihre langzeitliche Tauglichkeit in einem Unternehmen hin zu prüfen. Neben der Überprüfung der Persönlichkeit werden jedoch auch Plattformen, wie LinkedIn, genutzt, um ein Job-bezogenes Bild eines Arbeitnehmers zu erlangen, wobei davon ausgegangen wird, dass LinkedIn in Zukunft Resümees auf Papier ersetzen könnte. Bereits ein Drittel aller US-Arbeitgeber führen an, dass sie mit geringerer Wahrscheinlichkeit Personen einstellen, welche über keinen digitalen Fußabdruck verfügen.

Zwar dürfen Arbeitgeber nur einstellungsrelevante Informationen nutzen, welche sie über Bewerber:innen finden, jedoch gibt es keine definierten Grenzen oder ein kontrollierendes Organ, welches diesen Ablauf überwacht. Typischerweise werden Entscheidungen, welchen Cybervetting zugrunde liegt, mit wenig bis keiner organisatorischen Anleitung durchgeführt. So berichtet eine Human-Ressource-Fachkraft in einer US-amerikanischen Umfrage, dass es sie abschreckt, wenn eine Person auf einem Bewerbungsfoto unfreundlich aussieht. Dies zeigt, wie Emotionen der bearbeitenden Personaler:innen in Verbindung mit dem steigenden Zugriff auf persönliche Informationen einen erheblichen Einfluss auf die Wahl von Kandidat:innen haben. Diese Willkür bei der Bewertung von Bewerber:innen und die Unklarheit für deren nötige Voraussetzungen sorgt dafür, dass die in immer größeren Mengen vorhandenen Informationen über eine Person schwieriger in relevant und irrelevant zu unterteilen sind, wobei die Persönlichkeit eine größere Rolle spielt als beispielsweise die Intelligenz der Bewerber:innen. Aufgrund der größer werdenden Fülle an vorhandener Information wird das Bild verändert, das ein (potentieller) Angestellter erfüllen muss. So gibt es eine Verlagerung der Erwartung von Unternehmen, in welcher Weise Bewerber:innen und Arbeitnehmer:innen Informationen über die eigene Person managen sollen, aufgrund der wachsenden Selbstverständlichkeit, diese im Internet zu finden.

Nach dem Allgemeinen Gleichbehandlungsgesetz gibt es zwar allgemein Gesetze gegen Diskriminierung am Arbeitsplatz, jedoch ist die rahmenlose Vorgehensweise des Cybervettings in Deutschland noch nicht an Regeln gebunden. Zwar wird als ein Teilaspekt des Cybervettings die gesteigerte Effizienz des Bewerbungsverfahrens genannt, jedoch ist diese Verbesserung nicht nachgewiesen. So kann es ebenfalls sein, dass Cybervetting durch einen erhöhten Arbeitsaufwand und einer eventuellen Fehlleitung des Entscheidungsprozesses die Produktivität senkt und somit für ein Unternehmen Nachteile hinsichtlich Finanzen und Arbeitsklima bietet. Ein weiteres Problem ist, dass die Online-Präsenz der eigenen Person leicht zu beeinflussen und somit leicht zu verfälschen ist. So kann eine Person genau das Bild vermitteln, welches für ein Unternehmen am attraktivsten ist, auch wenn die angegebenen Daten nicht korrekt sind. Das Entfernen von Red Flags hat hierbei sogar größeren Einfluss als das Hinzufügen von positiven Informationen, da erstere in der Evaluation einer Person stärker gewichtet werden. Zwar geben Studien Hinweise darauf, dass Cybervetting eine wertvolle Ergänzung zu herkömmlichen Methoden ist, jedoch weisen sogar diese Studien teilweise gegensätzliche Ergebnisse auf, was am Nutzen von Cybervetting zweifeln lässt. Zusammenfassend lässt sich sagen, dass Cybervetting eine wichtige Rolle bei Entscheidungen für oder gegen eine Einstellung oder eine dauerhafte Beschäftigung spielen kann. Daher empfiehlt sich für jeden Menschen der sich (zukünftig) auf dem Arbeitsmarkt befindet, eine Auseinandersetzung mit der eigenen digitalen Identität aus der Perspektive des Cybervettings. Neben der Erlangung eines Bewusstseins für die Wirkung der eigenen digitalen Identität, ergibt sich hierbei die Chance, durch geeignete Änderungen, auf dem Arbeitsmarkt positiv herauszustechen.

Profiling

Profiling ist definiert als nutzbare Erstellung des Gesamtbildes einer Persönlichkeit für bestimmte Zwecke – z. B. zur Arbeitsvermittlung.

Berufliches Profiling im Speziellen meint dabei die Sammlung und Auswertung von Daten einer Person zum Abgleich einer zu besetzenden Stelle. Bei der zugehörigen Datensammlung spricht man vom Kandidat:innenprofil. Es werden möglichst alle relevanten Facetten erfasst und analysiert. Daraus entstehen Ergänzungen für das Profil. Diese sog. Merkmale sind Eigenschaftskategorien (z. B. Teamfähigkeit, Führungskompetenz, etc.), welche sich je nach Art des Profilings und Ziel des Unternehmens unterscheiden. Sie liefern wichtige Informationen für den Entscheidungsprozess.

Ziel des beruflichen Profilings ist die Steigerung der Produktivität des Auswahlprozesses bei mehreren Kandidat:innen. Außerdem kann die gesamte Produktivität eines Unternehmens durch Profiling, auch von Bestands-Mitarbeiter:innen, gesteigert werden. Durch Evaluation aller verfügbarer Ressourcen, wozu auch Mitarbeiter:innen gehören, können die Leistungsfähigkeit und Kompetenzen so ausgewählt und zugeteilt werden, dass beispielsweise die Innovationsfähigkeit und Kundenorientierung maximiert und optimiert werden.

„Kompetenz" meint hierbei nach Definition des Rates der Europäischen Union die nachgewiesene Fähigkeit, Kenntnisse, Fertigkeiten sowie persönliche, soziale und/oder methodische Fähigkeiten in Arbeits- oder Lernsituationen und für die berufliche und persönliche Entwicklung zu nutzen.

In einer Studie konnte gezeigt werden, dass Unternehmen, die besonderen Wert auf die Entwicklung und Bindung von Mitarbeiter:innen legen, im Vergleich zu durchschnittlichen Unternehmen einen höheren Marktwert pro Mitarbeiter aufweisen, was durch eine gezielte Auswahl und Verteilung von Personal begünstigt wird.

Der Schlüssel zum erfolgreichen Profiling liegt darin, geeignete Merkmale zu identifizieren. Ermittlungsgrundlage der Merkmale können Wohnort, Musikgeschmack oder Freizeitgestaltung sein. Es lassen sich allerdings auch abstraktere Informationen ermitteln, wie Werte, Wünsche oder Lebenseinstellung. All diese Daten können zur Erstellung eines ganzheitlichen Profils einer Person genutzt werden, welches zusätzlich die Bewertung der jeweiligen Merkmale umfasst. Bei der Erstellung eines Bewerberprofils werden die formalen Qualifikationen, wie Schulabschluss, Ausbildung, bisherige Tätigkeiten etc. als auch die nicht-formalen Kompetenzen, wie Motivation oder Lernbereitschaft sowie Kenntnisse und Fähigkeiten aufgelistet, welche im Rahmen von Zusatzqualifikationen, ausgeübten angelernten Tätigkeiten, außerberuflichen Interessensgebieten oder ehrenamtlichen Engagement erworben wurden. Diese häufig zunächst unstrukturierten Daten sollen sinnvoll zusammengeführt werden, so dass unterschiedliche berufliche Einsatzmöglichkeiten durch Potentialanalysen und -beratungen aufgezeigt und weitere Beratungen (z. B. bzgl. beruflicher Qualifikationsmöglichkeiten, Coachingmaßnahmen, beruflicher Perspektiv-Seminare u.ä.) wo möglich und nötig passgenau angeboten werden können.

Zur Sammlung benutzerbezogener Daten dienen gleichermaßen Soziale Netzwerke und Medien. Diese regen zur interpersonellen, horizontalen und gegenseitigen Kommunikation an, wodurch zwangsläufig Daten angehäuft werden. Online-Content, beispielsweise YouTube-

Videos, Kommentare und Tweets sowie Online-Verbindungen, wie Freundschaften, Follows, Erwähnungen etc. können von Programmen durchsucht und für eine Vielzahl an Zwecken, wie der Erstellung und Erweiterung von Nutzerprofilen sowie Verhaltensvorhersagen verwendet werden.

Hierzu werden sogenannte Data- oder Web-Crawler genutzt. Dazu gehören Programme, die in der Lage sind, iterativ und automatisch Webseiten herunterzuladen und Internetadressen des zugrundeliegenden Codes abzurufen.

Ein solcher Crawler kann mit einer Homepage „gefüttert" werden und alle Unterseiten und Verlinkungen speichern. Fortgeschrittene Crawler können hierbei auch die gefundenen Ergebnisse priorisieren und Dubletten gesammelter Internetadressen ignorieren. Aufgrund der Tatsache, dass Benutzerinformationen sowie von Benutzer:innen generierter Inhalt öffentlich zugänglich sind, eine Vielzahl von möglichen Privatsphäre-Einstellungen nicht verwendet werden und des Fehlens einer zentralen Kontrollinstanz, können Plattformen und Anwendungen weitläufig überwacht werden. Benutzer:innen werden sogar ermutigt persönliche Details preiszugeben und somit dauerhafte und durchsuchbare Informationen zu generieren. Allein die Interaktionen mit anderen Nutzern und die Inhalte auf sozialen Plattformen enthüllen Aspekte der Persönlichkeit von Nutzer:innen, wodurch diese passiv ihre eigene digitale Identität erschaffen. Dieser Sachverhalt ist bereits Gegenstand einiger Studien, welche Hinweise darauf geben, dass Personen ihr Verhalten in der realen Welt auf ihr online Verhalten übertragen, was das Profiling von Personen über ihre digitalen Identitäten zu einem effektiven Mittel werden lässt.

Das Durchsuchen dieser Informationen mit Hilfe der erwähnten Crawler ist bereits durch einfachste technische Aufbauten möglich. So genügt ein Computer mit 4 GB RAM und einem Breitband-Internetanschluss, um sensible persönliche Informationen zu extrahieren. Um eine zuverlässige und aus realen Daten bestehende Sammlung zu ermöglichen, muss auf die Qualität der gesammelten Informationen geachtet werden. Hierzu müssen drei Punkte berücksichtigt werden: Der Speicherort der Daten, an denen diese eingesammelt werden können, muss bekannt sein. Eine Vorverarbeitung der Daten muss gegeben sein, um veraltete oder unnütze Informationen herauszufiltern. Außerdem ist eine weitere Verarbeitung der Daten sinnvoll, um zielgerichtete Analysen einer Person erstellen zu können.

Unter anderem kann dabei auch auf Verbindungen innerhalb und zwischen den Datensätzen geschaut werden, um etwaige Korrelationen aufzudecken.

All diese Daten können ohne die Zustimmung der Nutzer:innen gesammelt und ausgewertet werden.

Auf diesen Fakt berufen sich viele Organisationen, um das Profiling von Personen zu rechtfertigen. Aus den Daten von Personen, welche dem Prozess des Profilings unterzogen werden, können Kompetenz-Matrizen erstellt werden, welche einer Person in jedem Kompetenzbereich einen festen Wert zuordnet, welcher mit den Werten aus gleichen Kompetenzbereichen von anderen Personen verglichen werden kann. Kompetenzbereiche können dynamisch angepasst werden und umfassen beispielhaft Führungskompetenz, Vertrauenswürdigkeit, Belastbarkeit, etc.

Im beruflichen Umfeld kann Profiling Arbeitgeber mit nützlichen Informationen über den psychologischen Zustand (potentieller) Mitarbeiter:innen bzw. deren Persönlichkeitseigenschaften versorgen. Es können dabei sogar psychologische Charakterzüge offengelegt werden, wie Introvertiertheit, soziale und persönliche Frustration, gespaltene Loyalität sowie Narzissmus. Diese Ausweitung der Überwachung auf Kommunikation und soziale Interaktionen von (potentiellen) Angestellten bringt die Chance mit sich,

dass sich diese an ein Unternehmen oder eine Institution anpassen und aktiv deren Werte auch in zwischenmenschlicher Kommunikation zu vertreten, um ein positiveres Bild des Unternehmens zu vermitteln.

Diese Überwachung birgt jedoch die Gefahr, dass sich Mitarbeiter:innen auch im privaten Bereich nicht frei entfalten können. Anschauungen entgegen der vorherrschenden Ideologie werden bereits als ein negatives Attribut einer Person zugeschrieben, was die Meinungsäußerung auch in politischen Bereichen beeinflussen oder unterbinden kann.

Die gesammelten Informationen auf denen Annahmen von Unternehmen oder Sicherheitseinrichtungen beruhen, können ebenfalls fehlerhaft oder sogar irreführend sein.

Hierdurch kann eine Person als potenziell gefährlich oder gänzlich unpassend für ein Unternehmen wirken, wodurch die Chancen auf eine mögliche Arbeitsstelle erheblich geschmälert werden.

Das Vorhersagen solcher Verhaltensmuster bzw. Verhalten allgemein wird als Predictive Profiling bezeichnet und wird gemäß der Definition des Europarates vor allem durch das Erstellen von Profilen zur Evaluation, Analyse und Vorhersage von Personalaspekten – wie Leistungsfähigkeit im Beruf, ökonomische Situation, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Position oder Bewegungen – charakterisiert.

Die Vorhersagbarkeit von Attributen oder Verhaltensmustern von Individuen sorgt dafür, dass diese bewertet und in Kategorien eingeteilt werden. Diese Kategorien, in die alle Individuen durch den Prozess des Profilings eingeordnet werden, scheinen immer wichtiger als die einzelnen Personen selbst zu werden, was einen Verlust der Individualität nach sich zieht. Die Gefahr der Stigmatisierung von Personen, die einmal durch Profiling in eine negative Kategorie eingeordnet wurden, ist besonders hoch. Das Bundesverfassungsgericht hat geurteilt, dass polizeiliches Profiling, die sogenannte Rasterfahndung, ein höheres Risiko bedeutet, Ziel von weiteren strafrechtlichen Ermittlungen und somit öffentlicher Stigmatisierung zu werden. Bei dieser Sonderform des Profilings werden aus einer Reihe von Datenquellen Informationen beschafft, um diese nach vordefinierten Eigenschaften zu filtern, um so eine breite Masse an Menschen analysieren zu können. Studien belegen, dass die weitreichende Sammlung von persönlichen Informationen soziale Ungerechtigkeit, Diskriminierung und Vorurteile gegen politische oder ethnische Minderheiten sowie andere benachteiligte Gruppen erhöht. Beim Profiling ist besonders gefährlich, dass aus scheinbar anonymen und harmlosen Informationen sensitive Daten ermittelt werden können. Es ist relativ leicht eine Person anhand dieser Daten zu erkennen, selbst nachdem Schlüsselattribute wie Name und Adresse entfernt wurden; z. B. durch Nutzung der Browserhistorie. Allein durch diese Tatsache könnte bereits die freie Meinungsäußerung eingeschränkt werden, da eine scheinbar anonyme Meinungsäußerung mit etwas Aufwand an eine spezifische Person gekoppelt werden kann.

Beispiel für eine Software zur weiteren Verarbeitung von Profiling-Daten ist ein System der Universität Siegen. Dieses besteht aus einer Job-Profiling-Datenbank, einem Kompetenz-Profiling-System sowie einer grafischen Benutzeroberfläche, für einen direkten Zugang zu den verarbeiteten Daten. Die Datenbank besteht aus den von einer Institution erstellten Stellenprofilen, den Mitarbeiter:innen-Profilen sowie den Bewerber:innen-Profilen.

In den beiden zuletzt genannten Profiltypen werden Personen durch ein hierarchisches Profil-Ranking analysiert und nach Fähigkeiten und Leistungen in ihren jeweiligen Arbeitsbereichen eingestuft. Aus den Stellenprofilen können gezielt benötigte Kompetenzen extrahiert werden, welche im Prozess des Kompetenz-Mappings mit den Daten aus den eingestuften Mitarbeiter:innen- und Bewerber:innen-Profilen verglichen werden können. Beim Mapping werden die Ergebnisse der Evaluation aller Personen (Mitarbeitende oder Bewerbende) in einer Personen-Matrix aufgelistet. Mit einer Gewichtungs-Matrix werden die Eigenschaften jeder Person nach Wichtigkeit besagter Eigenschaft mit einem höheren Wert versehen, um dieser Eigenschaft ein höheres zahlenmäßiges Gewicht zu verleihen. Die Resultate werden in einer Ergebnis-Matrix dargestellt. Je besser eine Kompetenz bei einer Person eingestuft wurde – und sofern diese durch die Gewichtungs-Matrix vorteilhaft gewichtet wurde – desto kompetenter gilt diese Person im Endeffekt in einer bestimmten Position. Bei der Profil-Bewertung können die Ergebnisse der Analysen beurteilt und ausgewertet werden. Dies, sowie die Festlegung der Schwerpunkte der Gewichtungs-Matrix, werden dabei von Spezialist:innen und geschultem Fachpersonal durchgeführt.

Ziel dieser Software ist es, durch ein dynamisches Feedback sowie Anpassungen der Positionen von Mitarbeiter:innen und Bewerber:innen einer Institution die Effektivität und Effizienz zu steigern (Abbildung 4).

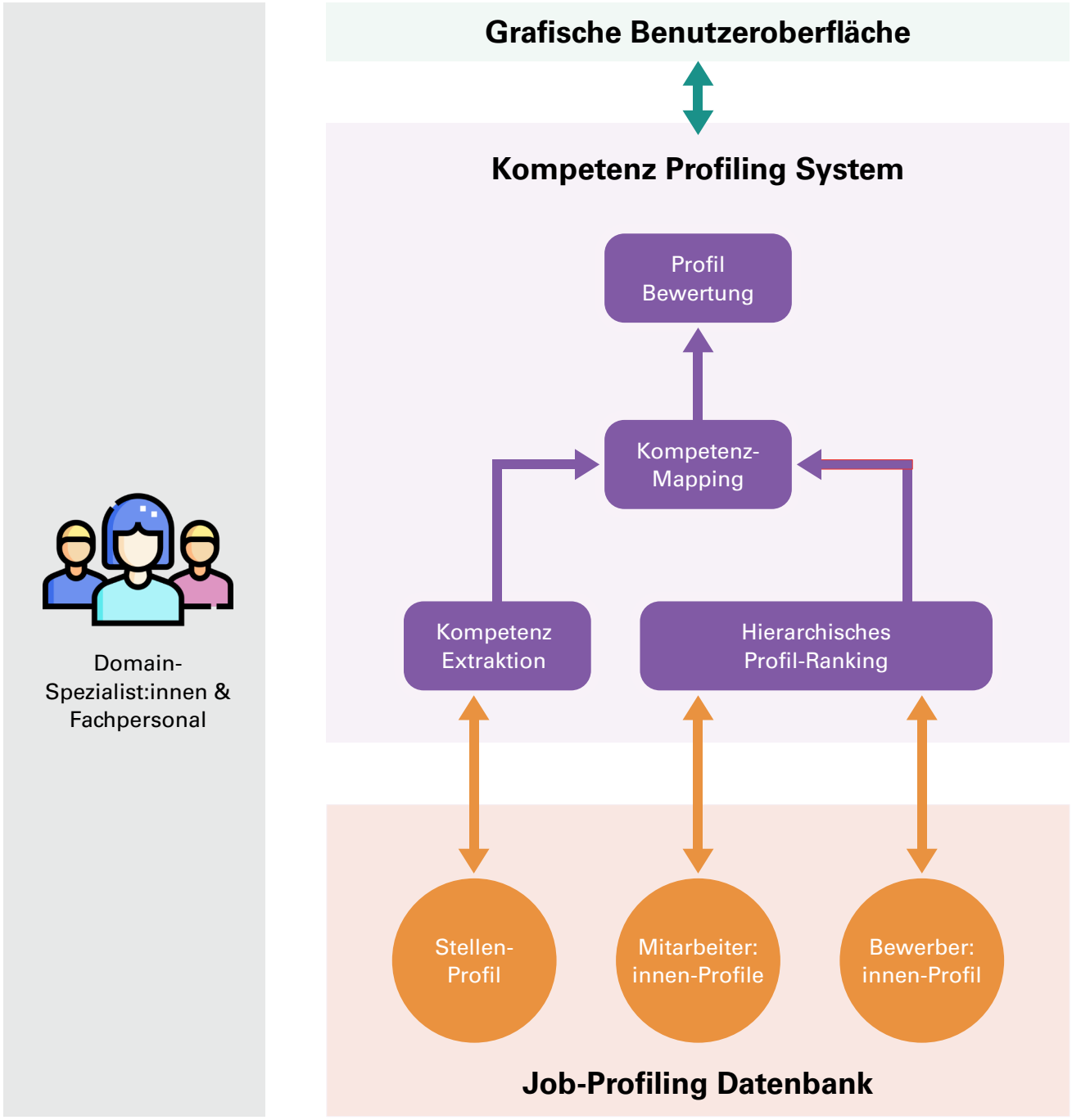


Abbildung 4: Schematische Darstellung einer Software zur weiteren Verarbeitung von Profilig-Daten (verändert nach Bohlouli et al. 2013) ◈

Neben dem beruflichen Profiling gibt es auch verschiedene andere Arten von Profiling. Darunter fallen politisches Profiling, Profiling im Marketing, Profiling im Gesundheitswesen, Sicherheitsprofiling sowie kulturelles Profiling.

Politisches Profiling extrahiert die politische Einstellung sowie den Beitrag zur gesellschaftlichen Gruppendynamik eines Individuums (z. B. Mitläufer, Unruhestifter, etc.).

Die Sammlung solcher Daten wird per Gesetz als eine außergewöhnliche Situation angesehen und durch viele internationale sowie nationale Vorgaben und Gesetze verhindert. Erlaubt sind solche Methoden nur, wenn dies im öffentlichen Interesse steht oder die Person, über die Informationen gesammelt werden sollen, zustimmt.

Profiling im Marketing, auch Kundenprofiling genannt, ist ebenfalls ein umfangreiches Analysewerkzeug. Hierbei werden Informationen darüber gesammelt, welche Dienste wann und in welcher Reihenfolge genutzt werden. Verknüpft mit Informationen über die Identität des Nutzers sowie eines demografischen Profils können Vorhersagen über zukünftiges Kauf- und Nutzungsverhalten gemacht werden.

Die Supermarktkette Target aus den Vereinigten Staaten hatte einen Schwangerschafts-Vorhersage-Wert erfunden, der nicht nur vorhersagen konnte, ob eine Kundin schwanger war, sondern auch, seit wann. Dies war möglich, da alle Nutzer:innen per Identifikationsnummer erfasst wurden und Daten wie Name, E-Mail-Adresse und Kreditkarteninformationen leicht zugeordnet werden konnten. So war es möglich, die Nutzungsverhalten aller Kund:innen zu überwachen und in Verbindung mit Daten aus anderen Quellen, wie dem spezialisierten Datensammler Acxiom genaue Vorhersagen über eine Schwangerschaft zu machen. Acxiom ist ein Unternehmen, welches Nutzer- und Umgebungsinformationen aus amtlichen Quellen zur Analyse von Kundenmarketing oder Sortimentplanung für andere Firmen zur Verfügung stellt und mit Daten von Firmen, wie beispielsweise Target ein vollständigeres Kundenbild erzeugen kann, als jedes der beiden Unternehmen alleine. Die Analyse ergab unter anderem, dass Schwangere ab einem bestimmten Zeitpunkt vermehrt unparfümierte Lotionen kaufen. Target konnte aus dem veränderten Konsumverhalten sogar schließen, wann ungefähr die Geburt anstand. Diese Informationen hätten dann für zielgerichtete Werbung eingesetzt werden können.

Profiling im Gesundheitswesen oder auch medizinisches Profiling kann genutzt werden, um aus persönlichen Daten sowie hauptsächlich der gesundheitlichen Historie eines Patienten/ einer Patientin das Risiko zu ermitteln, dass diese Person erneut erkrankt.

So gibt es z. B. in Malaysia eine Studie einiger Firmen, welche über Profiling versuchen die Kosten für die Krankenversicherung ihrer Angestellten zu reduzieren.

Sicherheitsprofiling umfasst hauptsächlich die Analyse von Mensch-Maschine-Schnittstellen, um Anomalien des biometrischen Nutzungsverhaltens (Interaktionen von Menschen mit Eingabegeräten wie Mäusen, Tastaturen, etc.) von Individuen zu erkennen, welche mit dem Zustand des Users verknüpft sind.

Deep Learning Algorithmen können aus diesem Verhalten Gefühlsprofile der jeweiligen Nutzer erstellen, um eine Risikoanalyse im Zuge der Sicherheit des Unternehmens durchzuführen. Hierzu können „Gated Recurring Units" (GRU) genutzt werden, welche ein mathematisches Verfahren für Erinnerungsprozesse in **rekurrenten*** neuronalen Netzwerken beschreiben.

* rekurrent = sich wiederholend

Hierbei werden Anomalien der Verhaltensweise einer Person mit dem normalen Verhalten derselben Person verglichen, um präzise Analysen des Gemütszustandes zu ermöglichen.

GRUs sind dabei einfache jedoch leistungsstarke Algorithmen, welche mit wenig Aufwand bereits präzise Ergebnisse erzielen können und damit viele andere Algorithmen von neuronalen Netzen übertreffen.

Kulturelles Profiling beschreibt die Sammlung von Daten zur Analyse der jeweiligen kulturellen Einstellung und Herkunft einer Person. Der kulturelle Hintergrund hat nach Studien zu kulturellen Unterschieden Einfluss auf Führungsstil, Identifikation mit einem Unternehmen, Engagement sowie das Verständnis von Arbeitssicherheit, berufliche Erfüllung, Zusammenarbeit und Veränderungsmanagement innerhalb eines Unternehmens.

Diese Art von Profiling kann dabei helfen, interkulturelle Zusammenarbeit zu stärken, um die positiven Einflüsse dieser zu nutzen. Gezielte Planung durch kulturelles Management kann dabei eine entscheidende Rolle spielen und zum Erfolg eines Unternehmens beitragen.

Zwischenmenschliche Kommunikation und Zusammenarbeit sind jedoch deutlich komplexer als beispielsweise das Kaufverhalten einer Person, weshalb diese Form des Profilings weiter erforscht werden muss, um rassistische und diskriminierende Analysen auszuschließen.

Leitfaden Handlungsempfehlungen

Die oben genannten Hintergrundinformationen sollen helfen, eine größere Sensitivität für die eigene digitale Identität zu erreichen. Nur wer einschätzen kann, wie seine eigene digitale Identität möglicherweise von anderen genutzt oder gar missbraucht werden kann, ist auch in der Lage, seine eigene digitale Identität so zu gestalten, dass sie für einen selbst von Vorteil ist.

Der folgende Leitfaden ist dazu gedacht. in kurzer und knapper Form die wichtigsten Dos and Don'ts zusammenzufassen, die sich aus dem Wissen über digitale Identitäten ableiten lassen.

Tipps zur Verwendung von sozialen Medien im privaten Bereich

- Überwache deine Online-Präsenz genau.
- Vor allem solltest du bei Social Media Posts aufpassen, da du hier schnell persönliche Informationen preisgeben könntest, die zukünftigen Arbeitgebern negativ auffallen können, sogenannte **„Red Flags“.** Zu diesen können Informationen zählen, wie religiöse Zugehörigkeit, Sexualität, Alkohol- oder Drogenkonsum, Gewalt, illegale Aktivitäten oder negative Einstellungen zur Arbeit. Hinterfrage deshalb jeden Eintrag, den du in Blogs, Foren, Kontaktnetzwerken u. ä. hinterlässt. Achte darauf, keine „politisch unkorrekten“ Äußerungen zu machen, auch wenn sie ironisch oder sarkastisch gemeint waren, da das leicht falsch interpretiert werden kann. Ein professioneller digitaler Fußabdruck wird mit einer Abwesenheit von Red Flags gleichgesetzt.
- Persönliche Daten, wie Adresse, Name, Telefonnummer, Bankdaten können auch Hackern als Angriffspunkt dienen, um dir zu schaden. **Diese Informationen können auch unbewusst oder im Hintergrund veröffentlicht werden.**
- **Verwende Einstellmöglichkeiten bezüglich deiner Privatsphäre**, um den Zugang zu Informationen zu beschränken, welche online über dich verfügbar sind.
- Du kannst auch die **Sichtbarkeit von Informationen** auf einen bestimmten Personenkreis **beschränken**, sodass z. B. nur Freunde deinen Post sehen können.
- Überlege dir, ob du **dein Profil auf öffentlich oder privat setzen** möchtest. Dies ist bei den meisten Plattformen möglich.
- **Weise Freunde und Bekannte darauf hin, wenn du nicht in Posts und Einträgen von Webseiten zu erkennen sein willst. Und frage Personen, die auf deinen Bildern zu sehen sind, ob sie mit der Veröffentlichung einverstanden sind.**

- **Überprüfe das Internet regelmäßig auf Einträge zu deiner Person**, denn auch Dritte können dich verunglimpfen, indem sie (wahre oder unwahre) Behauptungen veröffentlichen. Eine einfache Google-Suche kann hierbei schon viele Informationen liefern.

- **Wenn du negative Einträge im Web findest, versuche diese durch gezielte positive Einträge zu verdrängen.**

Tipps zur Darstellung im beruflichen Bereich

- **Informiere dich im Vorhinein über die Unternehmenskultur**, um deinen eigenen Online-Auftritt daran anzupassen. Verschiedene aktive Interessensbereiche werden gern gesehen. So wird es positiv gesehen, sich als physisch aktive und soziale Person im Internet zu präsentieren, wenn die Unternehmenskultur als „energetisch", „unterhaltsam" und „sozial" beschrieben werden kann – beispielsweise durch Beiträge zu Wanderungen, Campingausflügen oder Sportveranstaltungen.

- **Lade ein qualitativ hochwertiges Profilfoto hoch** – beispielsweise bei LinkedIn – in welchem du professionell und gepflegt aussiehst. Das Profilbild ist das Erste, was gesehen wird und ist essenziell für den ersten Eindruck. Ein Mangel an professionellen Bildern kann von Personalverantwortlichen bereits als Red Flag gewertet werden. Dein Ziel hierbei sollte es sein, freundlich und kompetent rüberzukommen. Vermeintlich lustige Schnappschüsse können kontraproduktiv sein.

- **Nutze deine Chance mit einem Kreativ-Profil, das positiv auffällt.** Im World Wide Web sind deiner Kreativität keine Grenzen gesetzt. Ob ein eigenes Pinterest-Board, ein YouTube-Kanal oder eine eigene Bewerbungsseite – nirgendwo kannst du potenzielle Arbeitgeber kreativer auf dich aufmerksam machen als im Internet. Soziale Netzwerke mit Karriereschwerpunkt eignen sich gut, um berufliche Fähigkeiten zu betonen. Hier kommt es auf den berühmten roten Faden an. Gib deinem Profil also systematisch Struktur. Erfahrungen und Kenntnisse sollten zu einem harmonischen Gesamtbild verpackt werden und mit denen in deiner Bewerbung gemachten Angaben übereinstimmen. Unterm Strich solltest du Expert:in in einem bestimmten Berufsfeld sein – der Allrounder mit Kenntnissen hier und einigen Erfahrungen dort ist meist leicht ersetzbar und deshalb weniger gefragt.

- **Benutze für Einträge und Posts in Foren und Chats weder deinen vollen Namen noch deine offizielle E-Mail-Adresse** oder andere Informationen, die aus deiner Bewerbung ersichtlich sind, also den Personalverantwortlichen vorliegen, um keine möglicherweise negativen Spuren im Internet zu hinterlassen.

- Eine Abwesenheit von Informationen über die eigene Person im Allgemeinen kann von Arbeitgebern ebenfalls bereits als Red Flag gedeutet werden. **Es sollten bewusst positive Informationen online geteilt werden, als Teil einer modernen Professionalität.**
Das erste Ergebnis ist nicht unbedingt

Tipps zum Umgang mit Werbung

das Beste: Ergebnisse bei Suchmaschinen im Internet werden eigentlich nach Relevanz angezeigt. Bezahlte Ergebnisse werden je nach der Menge an gezahltem Geld höher auf der Ergebnisliste sortiert, obwohl sie nicht zwangsweise die höchste Relevanz haben. Auch können Ergebnisse als relevanter angezeigt werden, wenn die in dem Suchergebnis enthaltenden Schlüsselwörter öfter auf der Seite vorhanden sind. **Achte auf die Qualität der Ergebnisse.** Gekaufte Ergebnisse sind meist mit dem Wort „Sponsored" oder „Anzeige" gekennzeichnet.

- Werbung im Internet ist an die digitale Identität angepasst. **Personalisierte Werbung kann bei Google oder Apple deaktiviert werden**, sodass man über die zugehörige Werbe-ID nur zufällige Werbungen angezeigt bekommt.

- **Verwende für die eigene Sicherheit, verbesserte Ladezeiten und zur Vermeidung von störender Werbung Applikationen zum Blockieren von Werbung** (Ad-Blocker). Nützlich ist es hierbei, mehrere zu verwenden, falls Firmen sich den Werbezugang über manche Ad-Blocker erkauft haben.

- **Lehne Cookies ab.** Achte darauf, dass die Ablehnen-Einstellung auch versteckt werden kann, jedoch ist diese per Gesetz gefordert, sodass du hierzu immer die Möglichkeit hast.

- **Lösche gelegentlich deinen Browser-Verlauf** oder lasse, durch die entsprechende Browsereinstellung, den Verlauf bei jedem Schließen des Browsers automatisch löschen.

- Sei dir bewusst, dass du durch Algorithmen in einer Informationsblase steckst, welche Informationen filtert und maßgeschneidert an dich anpasst. **Mit den oben genannten Punkten und deinem Nutzungsverhalten, kannst du die Algorithmen jedoch beeinflussen.**

Handlungsempfehlungen Zusammenfassung

Dos	Don'ts
Verwende Einstellungsmöglichkeiten bzgl. deiner Privatsphäre (Sichtbarkeit von Informationen beschränken, Profil auf privat setzen)	Vermeide Red Flags (Alkohol- oder Drogenkonsum, Gewalt, illegale Aktivitäten oder negative Einstellungen zur Arbeit, politisch unkorrekte Äußerungen)
Weise Freunde und Bekannte darauf hin, wenn du nicht in Posts und Einträgen von Webseiten zu erkennen sein willst	Veröffentliche keine persönlichen Daten (auf Dokumenten usw. im Hintergrund von Bildern & Videos, etc.)
Frage Personen, die auf deinen Bildern zu sehen sind, ob sie mit der Veröffentlichung einverstanden sind	Benutze für Einträge und Posts in Foren und Chats weder deinen vollen Namen noch deine offizielle E-Mail-Adresse
Überprüfe das Internet regelmäßig auf Einträge zu deiner Person	
Versuche negative Beiträge mit Positiven zu verdrängen	
Passe deine Online-Präsenz vor einer Bewerbung der Unternehmenskultur an	
Lade ein qualitativ hochwertiges Profilfoto hoch (Ziel hierbei sollte es sein, freundlich und kompetent rüberzukommen)	
Zeige dein Können & Interesse mit einem Kreativ-Profil (z. B. auf Pinterest oder YouTube)	
Es sollten bewusst positive Informationen online geteilt werden	
Achte auf die Qualität der Ergebnisse von Suchmaschinen	
Personalisierte Werbung sollte deaktiviert werden	
Verwende Ad-Blocker	
Lehne Cookies ab	
Lösche gelegentlich deinen Browser-Verlauf	

Literaturverzeichnis

Für diesen Leitfaden sind die folgenden Quellen verwendet worden.

Acxiom Corporation (2022): The Data Foundation for the World's Best Marketers. Online verfügbar unter https://www.acxiom.de/unternehmen/, zuletzt geprüft am 16.02.2023.

Agentur der Europäischen Union für Grundrechte (2007): Article 8 - Protection of personal data. Online verfügbar unter https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data#explanations, zuletzt geprüft am 02.01.2023.

Almahmoud, Sawsan; Hammo, Bassam; Al-Shboul, Bashar; Obeid, Nadim (2022): A hybrid approach for identifying non-human traffic in online digital advertising. In: Multimed Tools Appl 81 (2), S. 1685–1718. DOI: 10.1007/s11042-021-11533-4.

An, Mimi (2016): Why People Block Ads. And what it means for Marketers and Advertisers. Hubspot. Online verfügbar unter https://blog.hubspot.com/marketing/why-people-block-ads-and-what-it-means-for-marketers-and-advertisers, zuletzt aktualisiert am 14.01.2020, zuletzt geprüft am 06.01.2023.

Anthes, Gary (2015): Data brokers are watching you. In: Commun. ACM 58, 2015 (1), S. 28–30.

Antidiskriminierungsstelle des Bundes (2007): Allgemeines Gleichbehandlungsgesetz (AGG). In: Volker Emmerich und Jürgen Sonnenschein (Hg.): Miete: De Gruyter. Online verfügbar unter https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/DE/publikationen/AGG/agg_gleichbehandlungsgesetz.pdf?__blob=publicationFile, zuletzt geprüft am 08.10.2022.

Attoresi, Massimo; Moraes, Thiago; Zerdick, Thomas (2020): Personal Information Management Systems. Online verfügbar unter https://edps.europa.eu/sites/default/files/publication/21-01-06_techdispatch-pims_en_0.pdf, zuletzt geprüft am 24.03.2023.

Backman, Christel; Hedenus, Anna (2022): Professional talk on cybervetting: Accounting for a contested practise. In: Acta Sociologica, 000169932210887. DOI: 10.1177/00016993221088741.

Berkelaar, Brenda L. (2014): Cybervetting, Online Information, and Personnel Selection. New Transparency Expectations and the Emergence of a Digital Social Contract. In: Management Communication Quarterly 28 (4), S. 479–506. DOI: 10.1177/0893318914541966.

Berkelaar, Brenda L. (2017): Different ways new information technologies influence conventional organizational practices and employment relationships: The case of cybervetting for personnel selection. In: Human Relations 70 (9), S. 1115–1140. DOI: 10.1177/0018726716686400.

Berkelaar, Brenda L.; Buzzanell, Patrice M. (2014): Cybervetting, Person–Environment Fit, and Personnel Selection: Employers' Surveillance and Sensemaking of Job Applicants' Online Information. In: Journal of Applied Communication Research 42 (4), S. 456–476. DOI: 10.1080/00909882.2014.954595.

Berkelaar, Brenda L.; Harrison, Millie A. (2016): Cybervetting: John Wiley & Sons, Inc.

Beuth, Patrick (2014): Big Data - Schwanger ohne digitale Spuren. Hg. v. Zeit Online, zuletzt geprüft am 07.11.2022.

Big Data Insider (2022): Was ist eine Gated Recurrent Unit (GRU)? Online verfügbar unter https://www.bigdata-insider.de/was-ist-eine-gated-recurrent-unit-gru-a-d07bda28c3535c198d783b16a35ed9bb/, zuletzt geprüft am 14.11.2022.

Bohlouli, Mahdi; Ansari, Fazel; Patel, Yogesh; Fathi, Madjid; Cid, Miguel Loitxate; Angelis, Lefteris (2013): Towards analytical evaluation of professional competences in Human Resource Management. In: IECON 2013 - 39th

Annual Conference of the IEEE Industrial Electronics Society. IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society. Vienna, Austria, 10.11.2013 - 13.11.2013: IEEE, S. 8335–8340.

Brandcom (2019): 5 Basic-Tipps für einen erfolgreichen Social Media Post. Online verfügbar unter https://www.brandcom.de/blog/5-basic-tipps-fuer-einen-erfolgreichen-social-media-post/, zuletzt geprüft am 16.01.2023.

Braun, Simone; Follwarczny, Dan; Heißler, Andreas (2022): Neue Kanäle – neue Daten: Die veränderte Rolle von Kundendaten im Handel. In: Thomas Breyer-Mayländer, Christopher Zerres, Andrea Müller und Kai Rahnenführer (Hg.): Die Corona-Transformation. Wiesbaden: Springer Fachmedien Wiesbaden, S. 133–159.

Brave Software Inc. (2015): The best privacy online. Browse privately. Search privately. And ditch Big Tech. Online verfügbar unter https://brave.com/, zuletzt aktualisiert am 2023, zuletzt geprüft am 10.02.2023.

Bump, Pamela (2022): The Death of the Third-Party Cookie: What Marketers Need to Know About Google's 2023 Phase-Out. HubSpot, Inc. Online verfügbar unter https://blog.hubspot.com/marketing/third-party-cookie-phase-out, zuletzt aktualisiert am 27.07.22, zuletzt geprüft am 15.01.23.

BVerfG, Beschluss des Ersten Senats vom 04.04.2006, Aktenzeichen - 1 BvR 518/02 -, Rn. 1-184,

Cahn, Aaron; Alfeld, Scott; Barford, Paul; Muthukrishnan, S. (2016): An Empirical Study of Web Cookies. In: WWW 2016, S. 891–901. DOI: 10.1145/2872427.2882991.

Camp, L. Jean (2004): Digital identity. In: IEEE Technol. Soc. Mag. 23 (3), S. 34–41. DOI: 10.1109/MTAS.2004.1337889.

CareerBuilder®: More Than Half of Employers Have Found Content on Social Media That Caused Them NOT to Hire a Candidate, According to Recent CareerBuilder Survey. Unter Mitarbeit von Ladan Nikravan Hayes. Online verfügbar unter https://press.careerbuilder.com/2018-08-09-More-Than-Half-of-Employers-Have-Found-Content-on-Social-Media-That-Caused-Them-NOT-to-Hire-a-Candidate-According-to-Recent-CareerBuilder-Survey, zuletzt geprüft am 08.10.2022.

Chan, Nicholas Khin-Whai; Siew-Hoong, Angela; Zainol, Zuraini (2020): Profiling Patterns in Healthcare System: A Preliminary Study. In: IJACSA 11 (4). DOI: 10.14569/IJACSA.2020.0110485.

Chung, Junyoung; Gulcehre, Caglar; Cho, KyungHyun; Bengio, Yoshua (2014): Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling. Online verfügbar unter http://arxiv.org/pdf/1412.3555v1.

Clauß, Sebastian; Köhntopp, Marit (2001): Identity management and its support of multilateral security. In: Computer Networks 37 (2), S. 205–219. DOI: 10.1016/S1389-1286(01)00217-1.

Crain, Matthew (2018): The limits of transparency: Data brokers and commodification. In: New Media & Society 20 (1), S. 88–104. DOI: 10.1177/1461444816657096.

Desai, Vaibhava (2019): Digital Marketing: A Review. In: International Journal of Trend in Scientific Research and Development (IJTSRD), S. 196–200. Online verfügbar unter https://www.ijtsrd.com/papers/ijtsrd23100.pdf.

Duden.de (Hg.) (2023): Profiling - Rechtschreibung, Bedeutung, Definition, Herkunft. Online verfügbar unter https://www.duden.de/rechtschreibung/Profiling, zuletzt geprüft am 05.11.2022.

Europäische Kommission (2021): on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework. Commission Recommendation. Unter Mitarbeit von Thierry Breton. Hg. v. Europäische Kommission. Europäische Kommission. Brüssel (C(2021) 3968). Online verfügbar unter file:///C:/Users/Perru/Downloads/C2021_3968_EN_ACT_part1_dNLKk3HM1tYtdlvGDYPq3Rtp6Jc_76610.pdf, zuletzt geprüft am 16.08.2022.

Europarat (2011): La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage. Recommandation CM/Rec(2010)13 adoptée par le Comité des Ministres du Conseil de l'Europe le 23 novembre 2010 et exposé des motifs. Strasbourg: Editions du Conseil de l'Europe (Recommandation / Conseil de l'Europe, Comité des Ministres, CM/Rec 2010,13). Online verfügbar unter https://rm.coe.int/16807096c3, zuletzt geprüft am 12.12.2022.

Europarat (2018): Convention 108+. Online verfügbar unter https://www.coe.int/en/web/data-protection/convention108-and-protocol, zuletzt geprüft am 02.01.2023.

Fernandez, Sébastien; Stöcklin, Marie; Terrier, Lohyd; Kim, Sowon (2021): Using available signals on LinkedIn for personality assessment. In: Journal of Research in Personality 93, S. 104122. DOI: 10.1016/j.jrp.2021.104122.

Fu, Kevin; Sit, Emil; Smith, Kendra; Feamster, Nick (2001): Dos and Don'ts of Client Authentication on the Web. In: IEEE Softw. 28 (3). DOI: 10.1109/MS.2011.67.

Gallego-Toledo, Juan-Maria (2015): Cultural profiling and a Chinese experience. In: JCHRM 6 (2), S. 120–132. DOI: 10.1108/JCHRM-09-2015-0014.

Ghostery inc. (2023): We make privacy easy. Browse the web safer, faster & with less annoying ads. Online verfügbar unter https://www.ghostery.com/, zuletzt aktualisiert am 2023, zuletzt geprüft am 10.02.2023.

Grassi, Paul A.; Garcia, Michael E.; Fenton, James L. (2017): Digital identity guidelines: revision 3. Gaithersburg, MD.

Grote, Saskia (2021): Wann ist die beste Zeit zum Posten auf Social Media? Hg. v. Meltwater. Online verfügbar unter https://www.meltwater.com/de/blog/beste-zeit-zum-post-social-media, zuletzt geprüft am 16.01.2023.

Gu, Yiquan; Madio, Leonardo; Reggiani, Carlo (2018): Data Brokers Co-Opetition. In: SSRN Journal (3), Artikel 74, 820-839. DOI: 10.2139/ssrn.3308384.

Gul, Sumeer; Ali, Sabha (2015): An Art of Driving Web Traffic to Web Sites: Search Engine Optimization (SEO). In: International Journal of Web Engineering and Technology 2 (1), S. 1–5.

Hansen, Marit; Meints, Martin (2006): Digitale Identitäten — Überblick und aktuelle Trends. In: DuD 30 (9), S. 543–547. DOI: 10.1007/s11623-006-0139-9.

Hassler, Marco (2021): Von Data-driven zu People-based Marketing. Erfolgreiche Digital Marketing Strategien in einer Privacy First Ära. S.l.: MITP. Online verfügbar unter https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=3017538.

heute im Bundestag (hib) (2022): Projekt „Digitale Identitäten". Inneres und Heimat/Antwort - 13.05.2022 (hib 235/2022). Zentner, Christian. elektronisch (Homepage). Online verfügbar unter https://www.bundestag.de/presse/hib/kurzmeldungen-894754, zuletzt geprüft am 16.08.2022.

Hildebrandt, Mireille; Koops Bert-Jaap; Vries, Katja de (2009): Where Idem-Identity meets Ipse-Identity. Conceptual Explorations. D7.14a. In: FIDIS (Future of Identity in the Information Society) EU-Projekt Deliverables. Network of Excellence. European Union, S. 1–49. Online verfügbar unter http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP7-del7.14b-idem-ipse-profiling-practices.pdf, zuletzt geprüft am 02.08.2022.

IHK München und Oberbayern (2022): Social-Media-Marketing – der große Leitfaden. Online verf|gbar unter https://www.ihk-muenchen.de/de/Service/Marketing-Vertrieb/social-media-marketing/, zuletzt geprüft am 16.01.2023.

ITU-T Recommendation X.1252, 30.04.2021: Baseline identity management terms and definitions. Online verfügbar unter https://handle.itu.int/11.1002/1000/14642, zuletzt geprüft am 28.07.2022.

DIN EN ISO/IEC 24760-1:2022-03, 28.03.2022: Informationstechnik_- Sicherheitsverfahren_- Rahmenwerk für Identitätsmanagement_- Teil_1: Terminologie und Konzept (ISO/IEC_24760-1:2019); Deutsche und Englische Fassung prEN_ISO/IEC_24760-1:2022.

Jacobson, Jenna; Gruzd, Anatoliy (2020): Cybervetting job applicants on social media: the new normal? In: Ethics Inf Technol 22 (2), S. 175–195. DOI: 10.1007/s10676-020-09526-2.

Jaquet-Chiffelle, David-Olivier; Benoist, Emmanuel; Haenni, Rolf; Wenger, Florent; Zwingelberg, Harald (2009): Virtual Persons and Identities. In: Kai Rannenberg (Hg.): The future of identity in the information society. Challenges and opportunities. Berlin, Heidelberg: Springer, S. 75–122.

Jechorek, Janina (2022): Neue Daten: Statistiken zur Social-Media-Nutzung in Deutschland. Hg. v. HubSpot, Inc. Online verfügbar unter https://blog.hubspot.de/marketing/social-media-in-deutschland, zuletzt geprüft am 16.01.2023.

King, Andrew B. (2008): Website optimization. Speed, search engine & conversion rate secrets. 1st ed. Beijing, Köln: O'Reilly. Online verfügbar unter https://www.websiteoptimization.com/wp-content/uploads/2022/08/conversion-rate-optimization.pdf, zuletzt geprüft am 24.03.2023.

Koch, Wolfgang (2022): Reichweiten von Social-Media-Plattformen und Messengern. In: ARD/ZDF-Forschungskommission (Hg.): ARD/ZDF-Onlinestudie, S. 471–478. Online verfügbar unter https://www.ard-zdf-onlinestudie.de/files/2022/2210_Koch.pdf, zuletzt geprüft am 16.01.2023.

LaCroix, Kenneth; Loo, Yin L.; Choi, Young B. (2017): Cookies and Sessions: A Study of What They Are, How They Work and How They Can Be Stolen. In: 2017 International Conference on Software Security and Assurance 2017 International Conference on Software Security and Assurance, S. 20–24. DOI: 10.1109/ICSSA.2017.9.

Larkina, Anna (2019): Data Collectors. Kaspersky. Securelist. Online verfügbar unter https://securelist.com/data-collectors/94339/, zuletzt aktualisiert am 23.10.2019, zuletzt geprüft am 29.09.2022.

Ludwig, Beate (2003): Revision von Profiling-Instrumenten. Abgleich vorhandener Instrumentarien (Vorstudie) und Entwicklung von allgemein verwendbaren Profiling-Instrumenten. Online verfügbar unter https://www.ams-forschungsnetzwerk.at/downloadpub/Revision_Profiling_Instrumente_ludwig_2003_dobischat.pdf.

McDonald, Steve; Damarin, Amanda K.; McQueen, Hannah; Grether, Scott T. (2021): The hunt for red flags: cybervetting as morally performative practice. In: Socio-Economic Review, Artikel mwab002. DOI: 10.1093/ser/mwab002.

McLachlan, Stacey; Mikolajczyk, Karolina (2022): 2023 Instagram Algorithm Solved: How to Get Your Content Seen. Hg. v. Hootsuite Inc. Online verfügbar unter https://blog.hootsuite.com/instagram-algorithm/, zuletzt geprüft am 16.01.2023.

Meta (2022): Kontrolliere deine Sichtbarkeit. Online verfügbar unter https://de-de.facebook.com/help/instagram/116024195217477/?helpref=hc_fnav, zuletzt geprüft am 16.01.2023.

Mitrou, Lilian; Kandias, Miltiadis; Stavrou, Vasilis; Gritzalis, Dimitris (2014): Social Media Profiling: A panopticon or omniopticon tool? Online verfügbar unter https://www.infosec.aueb.gr/Publications/2014-SSN-Privacy%20Social%20Media.pdf, zuletzt geprüft am 07.11.2022.

Mönke, Franz Wilhelm; Schäpers, Philipp (2022): Too early to call: What we do (not) know about the validity of cybervetting. In: Ind. Organ. Psychol. 15 (3), S. 334–341. DOI: 10.1017/iop.2022.51.

onpulson.de (Hg.) (2023): Berufliches Profiling - Onpulson Wirtschaftslexikon. Online verfügbar unter https://www.onpulson.de/lexikon/berufliches-profiling/, zuletzt geprüft am 07.11.2022.

Pahrmann, Corina; Kupka, Katja; Schwenke, Thomas; Ladwig, Wibke; Weinberg, Tamar (2020): Social Media Marketing. Praxishandbuch für Twitter, Facebook, Instagram & Co. 5. Auflage. Heidelberg, Ann Arbor, Michigan: O'Reilly; ProQuest.

Pande, Pratik V.; Tarbani, Nitesh M.; Ingalkar, Pavan V. (2014): A Study of Web Traffic Analysis. In: International Journal of Computer Science and Mobile Computing 3 (3), S. 900–907.

Papadopoulos, Panagiotis; Kourtellis, Nicolas; Markatos, Evangelos P. (2018): The Cost of Digital Advertisement: Comparing User and Advertiser Views. In: WWW '18: Proceedings of the 2018 World Wide Web Conference, S. 1479–1489. DOI: 10.1145/3178876.3186060.

Pfitzmann, Andreas; Hansen, Marit (2000-2010): A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. v.0.34. TU Dresden. Online verfügbar unter http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, zuletzt geprüft am 01.08.2022.

Pongratz, Hans J. (2021): Bewerbung als Risiko? Informationskontrolle auf dem digitalisierten Arbeitsmarkt. In: WISO Direkt. Online verfügbar unter https://www.fes.de/referat-demokratie-gesellschaft-und-innovation/artikelseite-dgi/bewerbung-als-risiko, zuletzt geprüft am 08.10.2022.

Pooranian, Zahra; Conti, Mauro; Haddadi, Hamed; Tafazolli, Rahim (2021): Online Advertising Security: Issues, Taxonomy, and Future Directions. In: IEEE Commun. Surv. Tutorials 23 (4), S. 2494–2524. DOI: 10.1109/COMST.2021.3118271.

Ramirez, Edith; Brill, Julie; Ohlhausen, Maureen K.; Wright, Joshua D.; McSweeny, Terrell (2014): Data Brokers. A Call for Transparency and Accountability. Federal Trade Commission. Online verfügbar unter https://www.ftc.gov/

reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014, zuletzt geprüft am 15.10.2022.

Rat der Europäischen Union (2017): Empfehlung des Rates vom 22. Mai 2017 über den Europäischen Qualifikationsrahmen für lebenslanges Lernen und zur Aufhebung der Empfehlung des Europäischen Parlaments und des Rates vom 23. April 2008 zur Einrichtung des Europäischen Qualifikationsrahmens für lebenslanges Lernen. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017H0615(01)&from=EN.

Rouse, Craig (2022): What is 2nd Party Data? Here's Your Answer. Tealium. Online verfügbar unter https://tealium.com/blog/data-strategy/what-is-2nd-party-data-heres-your-answer/, zuletzt aktualisiert am 28.03.2022, zuletzt geprüft am 16.12.2022.

Schawbel, Dan (2011): 5 Reasons Why Your Online Presence Will Replace Your Resume in 10 years. Online verfügbar unter https://www.forbes.com/sites/danschawbel/2011/02/21/5-reasons-why-your-online-presence-will-replace-your-resume-in-10-years.

Schelenz, Bernhard (2022): Arbeitgeberkommunikation neu denken | Crosswater Job Guide. HR als Ermittler: Mit Candidate Profling das Recruiting erfolgreich machen. Crosswater Job Guide. Online verfügbar unter https://crosswater-job-guide.com/archives/60688/arbeitgeberkommunikation-neu-denken, zuletzt geprüft am 07.11.2022.

Schermer, Bart W. (2011): The limits of privacy in automated profiling and data mining. In: Computer Law & Security Review 27 (1), S. 45–52. DOI: 10.1016/j.clsr.2010.11.009.

Schroeder, Amber N.; Cavanaugh, Jacqulyn M. (2018): Fake it 'til you make it: Examining faking ability on social media pages. In: Computers in Human Behavior 84, S. 29–35. DOI: 10.1016/j.chb.2018.02.011.

Shiller, Benjamin; Waldfogel, Joel; Ryan, Johnny (2018): The effect of ad blocking on website traffic and quality. In: The RAND Journal of Economics 49 (1), S. 43–63. DOI: 10.1111/1756-2171.12218.

Slynchuk, Andiry (2021): Big brother brands report: which companies might access our personal data the most? Clario. Online verfügbar unter https://clario.co/blog/which-company-uses-most-data/, zuletzt aktualisiert am 22.06.2021, zuletzt geprüft am 29.09.2022.

Soha, Charlie; Yua, Sicheng; Narayanana, Annamalai; Duraisamya, Santhiya; Chena, Lihui (2019): Employee Profiling via Aspect-based Sentiment and Network for Insider Threats Detection.

Sponheuer, Birgit (2012): Employer Branding als Bestandteil einer ganzheitlichen Markenstrategie. 1. Aufl. Wiesbaden: Gabler Research.

Tamblé, Melanie (2020): Die besten Social-Media-Zeiten. Dein Social-Media-Zeitplan auf einen Blick. Hg. v. Adenion GmbH. Online verfügbar unter https://www.blog2social.com/de/blog/infografik-die-besten-zeiten-fuer-social-media-beitraege/, zuletzt geprüft am 16.01.2023.

Thelwall, Mike (2001): A web crawler design for data mining. Online verfügbar unter https://journals.sagepub.com/doi/epdf/10.1177/016555150102700503, zuletzt geprüft am 19.11.2022.

Velagapudi, Sai Lahari; Gupta, Himanshu (2019): Privacy, Security Of Cookies In HTTP Transmission. In: 2019 4th International Conference on Information Systems and Computer Networks (ISCON). DOI: 10.1109/ISCON47742.2019.

We Are Social; Hootsuite (2022): Digital 2022 Germany. Online verfügbar unter https://datareportal.com/reports/digital-2022-germany, zuletzt geprüft am 16.01.2023.

Wiedmann, Klaus-Peter; Buxel, Holger; Walsh, Gianfranco (2002): Customer profiling in e-commerce: Methodological aspects and challenges. In: J Database Mark Cust Strategy Manag 9 (2), S. 170–184. DOI: 10.1057/palgrave.jdm.3240073.

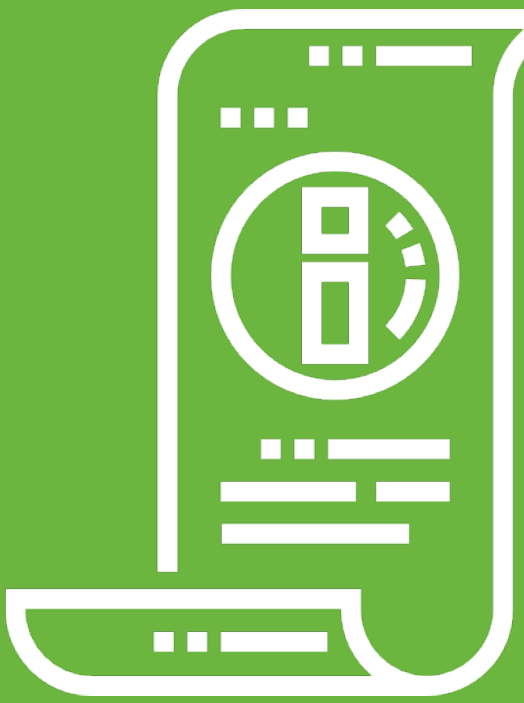
Wilcox, Annika; Damarin, Amanda K.; McDonald, Steve (2022): Is cybervetting valuable? In: Ind. Organ. Psychol. 15 (3), S. 315–333. DOI: 10.1017/iop.2022.28.

Yokoyama, Marcos Hideyuki (2016): How social network sites (SNS) have changed the employer–employee relationship and what are the next challenges for human resource (HR)? In: REGE - Revista de Gestão 23 (1), S. 2–9. DOI: 10.1016/j.rege.2015.11.001.

Impressum

Maßnahmen zur Verankerung von Digitalisierung und Nachhaltigkeit im Studiengang

„Sustainable Engineering and Management“



Förderprojekt digiSEM im Rahmen des Wettbewerbs Curriculum 4.0.nrw

Projektinformationen:
Förderprojekt: „Curriculum 4.0.nrw“, Wettbewerb zur Weiterentwicklung der bestehenden Hochschulcurricula dahingehend, dass Medienkompetenz und fachspezifische digitale Kompetenz stärker verankert werden.

Projektleitung: Prof. Dr. Heike Beismann, Westfälische Hochschule, Münsterstraße 265, 46397 Bocholt, heike.beismann@w-hs.de, Tel.: 02871/2155-944
Projektdurchführung: Matthias Fischer
Projektbeteiligte:
Alina Stock, Phil Martens, Darren Ajuzie
Förderer: Westfälische Hochschule gemeinsam mit MKW und DH.NRW
Projektzeitraum: 1.4.2022 bis 31.3.23

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

ORCA.nrw
Das Landesportal für Studium und Lehre.

DIGITALE HOCHSCHULE NRW

Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen