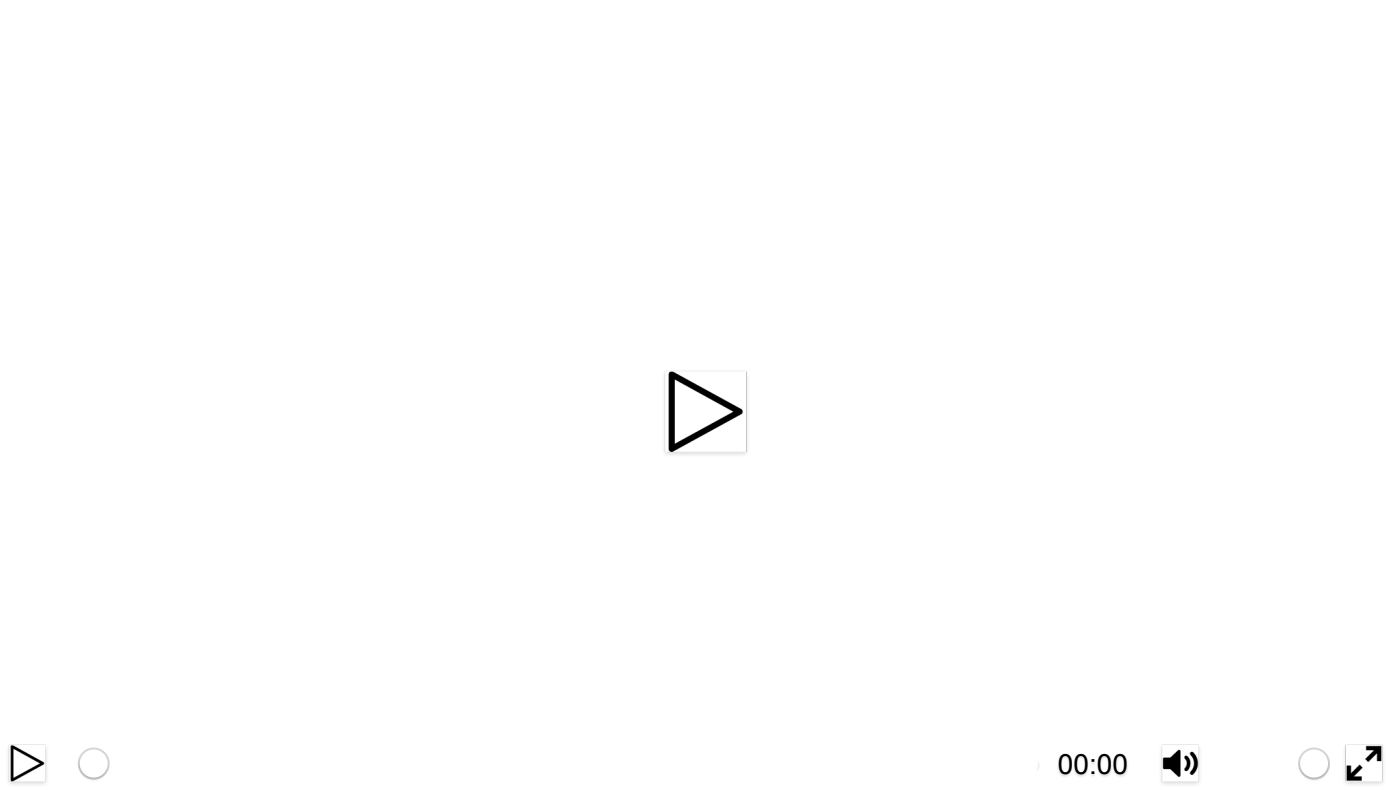
Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Baden-Württemberg

ALGORITHMEN

#seiunberechenbar ... beim Suchen & Finden



Jede Suchanfrage verrät etwas über unser Leben. Wie Suchmaschinen arbeiten und was man tun kann, um seine persönlichen Daten zu schützen, zeigen wir hier.

Das Internet bietet Millionen von Websites, Inhalten und Möglichkeiten. Um sich in diesem Informations-Dschungel zurechtzufinden, nutzen fast alle Verbraucher Suchmaschinen. Doch was uns meistens nicht bewusst ist: Während wir Suchanfragen stellen, sammeln die meisten der verwendeten Suchmaschinen unsere Daten und erstellen mithilfe von Algorithmen Profile über uns. Bereits bei der Zusammenstellung der Suchergebnisse werden zuvor gesammelte Daten und Profile berücksichtigt, so dass je nach Nutzer unterschiedliche Suchergebnisse angezeigt werden können.

Denn die meisten Suchmaschinen – oder auch Sprachassistenten wie "Alexa" von Amazon, Apples "Siri" oder der "Google Assistant" – sind zwar kostenlos. Doch auch sie müssen sich finanzieren. Das tun sie unter anderem über die persönlichen Daten ihrer Nutzer. Sie sammeln sie, um beispielsweise

zielgerichteter Werbung anzuzeigen, die den jeweiligen Nutzerbedürfnissen so genau wie möglich entsprechen. Beispielsweise können sich Suchmaschinen wie Google folgender Daten bedienen:

- Wonach jemand wann und von wo aus gesucht hat;
- Wann und wie häufig man Anfragen stellt;
- Von welcher Art Gerät und welchem Betriebssystem aus man sucht;
- Welche Webseiten man vorher und nachher ansteuert;
- Wie lange man sich auf den Webseiten aufhält, mit welchem Ergebnis man eine Webseite verlässt (Kommentar, Kauf, Bestellung, Download, u.a.) und wann man den Besuch der Webseite abgebrochen hat;
- Welche Zahlverfahren und Online-Bezahldienste man in Webshops benutzt (z.B. Giropay, Paydirekt, Paypal);
- Ob und wie Social-Media-Plattformen genutzt werden;
- In welcher Gegend jemand sich normalerweise aufhält und unterwegs ist;
- Welche Bewegungsprofile über den Nutzer bekannt sind;
- Welche Daten offline für den Benutzer bekannt sind (Einkaufskarten wie z.B. Payback, ec-Karten und Kreditkartennutzung, Online-Bezahldienste in Web).

Möglich wird das unter anderem durch sogenannte Cookies, Tracking-Tools und neuartige Technologien zur Nutzerverfolgung (Fingerprinting u.a.). Cookies sind kleine, textbasierte Dateien, die der Browser beim Besuch einer Webseite ablegt. Sie speichern das Verhalten des Nutzers, etwa wo er klickt oder welche Daten er eintippt. Wie oft war ein Nutzer bereits auf der Seite und welche Produkte hat er gekauft? Wie häufig kommt er wieder? Für welche Seiten hat er sich interessiert? Diese Fragestellungen können mit weit verbreiteten Web-Analyse-Tools wie Webtrekk, Google Analytics oder Adobe Analytics über das Setzen von Cookies beantwortet werden. Einige Cookies löschen sich automatisch, andere bleiben und horten so ganze Berge von Verhaltens-Daten.

Nun kommen Algorithmen ins Spiel: Beim nächsten Webseitenbesuch liefert der Browser die gesammelten Informationen automatisch an den Webserver der Seite, in dem Fall an die Suchmaschine. Diese nimmt die Daten und vergleicht sie mithilfe eines Algorithmus mit Tausenden anderer Datensätze, die sie auf dieselbe Art erhoben hat. Der Algorithmus macht dabei etwas, was Menschen nur schwerlich können – nämlich in den riesigen Datenmengen nach Mustern und vergleichbaren Merkmalen zu schauen. Auf diese Weise können die Betreiber von Suchmaschinen ein Profil erstellen und bei der Suchanfrage berücksichtigen.

Das könnte beispielsweise folgendermaßen lauten: Der Nutzer ist mit 98-prozentiger Chance weiblich, Mitte 40 und hat mit einer 83-prozentigen Chance mehrere Kinder. Sie surft mit Vorliebe abends mit ihrem Smartphone auf verschiedenen Web-Shops, teils zu Hause, teils bei Freunden und nutzt Social Media. Vormittags fährt sie in der S-Bahn zum Arbeitsplatz und holt mittags die jüngeren von der Schule mit dem Auto ab. Der Lieblingsitaliener ist im Nachbarort, der Supermarkt gleich um die Ecke. All das – und noch viel mehr – lässt sich tatsächlich aus unseren Suchanfragen ablesen, wenn Algorithmen sie verwerten und vergleichen.

Füttert der Nutzer also dieselbe Suchmaschine mit immer mehr Anfragen, ergibt sich nach und nach ein immer schärferes Bild für den Betreiber dieser Suchmaschinen. Und diese Daten sind wertvoll, denn nun bekommt der Nutzer personalisierte Werbung angezeigt, also Anzeigen, die genau seinen

Geschmack und seine Bedürfnisse treffen; nicht nur in den Suchergebnissen, sondern auch auf verlinkten Websites mit Werbeeinblendungen.

Manche Suchmaschinen gehen sogar noch einen Schritt weiter und lassen den Nutzer bewusst Wertungen zu den Ergebnissen abgeben. „Wenn Sie Google-Anwendungen nutzen, werden Sie gefragt: Sind Sie zufrieden mit den Ergebnissen? Mit Ihren Antworten helfen Sie Google sehr, denn anhand Ihrer Angaben kann der Konzern seine Anwendung verbessern", erklärt Dr. Jessica Heesen, die am Ethikzentrum der Universität Tübingen zur Ethik von Algorithmen forscht. „Das ist der einzige Weg, wie ein Algorithmus besser wird: Training durch Menschen. Sie sind sozusagen aufs Fehlermachen angewiesen, um besser zu werden."

Die Personalisierung hat natürlich auch Vorteile für uns Nutzer: Sie ist bequem. Doch auch Algorithmen können irren. Jeder kennt den Fall: Wir suchen zwei, drei Mal nach einem neuen Esstisch – und bekommen prompt monatelang Werbung für neue Esstische. Dass wir uns inzwischen schon längst entschieden und gekauft haben, wird vom Algorithmus nicht bemerkt.

Außerdem kann das Profil, das unbemerkt von uns erstellt wird, auch fehlerhaft sein. Zum Beispiel sind falsche Informationen mit eingeflossen, oder der Algorithmus hat sich in der Interpretation geirrt. Auf diese Auswertung haben wir nur begrenzten Einfluss.

Deswegen ist es wichtig, dass wir uns bewusstmachen, was bei Suchanfragen und beim Surfen im Netz passiert – und es gegebenenfalls gar nicht dazu kommen lassen. Wir zeigen Ihnen, wie.

So mache ich mich #unberechenbar beim Suchen & Finden

1. **Alternative Suchmaschinen nutzen, die keine Nutzerdaten sammeln**

Wer seinen Browser öffnet, dem wird in vielen Fällen automatisch Google als erste Anlaufstelle angeboten. Google ist weltweiter Marktführer unter den Suchmaschinen – auch, weil viele Menschen den Browser „Chrome" nutzen, der von Google stammt. Alternativ bieten sich hier als Browser-Programm beispielsweise die freie Alternative Firefox, Apples Safari oder Edge von Microsoft an.

In beinahe jedem Browser lässt sich jedoch die Startseite einstellen. Hier können Sie also auch Google-Alternativen eingeben. Einige davon setzen besonders auf den Schutz der persönlichen Daten ihrer Nutzer.

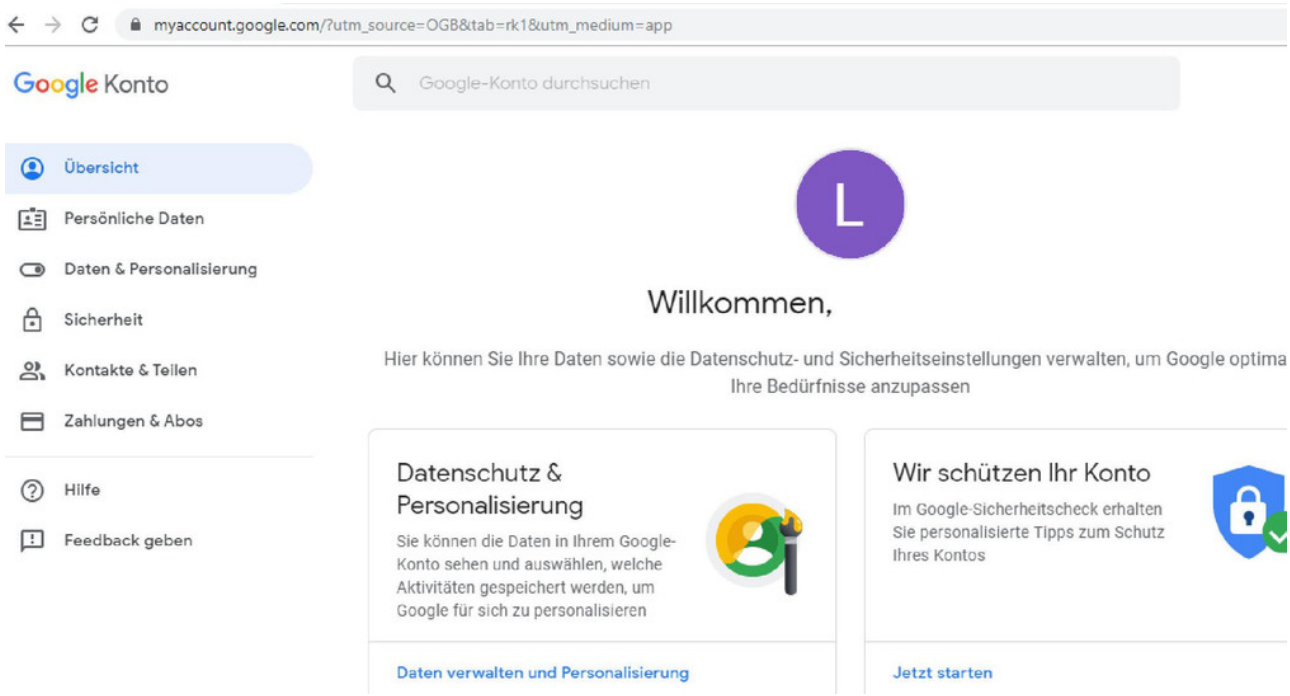
Metager ist ein gutes Beispiel aus Deutschland: Die Seite leitet Suchanfragen anonymisiert an verschiedene Suchmaschinen weiter und finanziert sich über nicht-personalisierte Werbung – ganz ohne Daten vom Nutzer zu sammeln. Ebenfalls beliebte Alternativen sind DuckDuckGo aus den USA und Startpage aus den Niederlanden, die auf den Algorithmus von Google setzt, allerdings ohne Speicherung der Nutzerdaten – sozusagen die datensparsame Variante zu Google.

2. **Die Suchmaschine so einstellen, dass man personalisierte Werbung vermeidet**

Wer trotzdem nicht auf Google mitsamt seinen unterschiedlichen Diensten verzichten möchte, sollte zumindest einige der Einstellungen der Suchmaschine anpassen. Dazu müssen Sie ein eigenes Konto bei Google erstellen – und sich dort einloggen. Dafür brauchen Sie eine Mailadresse – die aber nicht zwingend ihren Klarnamen umfassen muss. Eine Möglichkeit wäre, eine „Einweg"-Mailadresse, die eigens für diesen Zweck angelegt wird, zu nutzen.

Klicken Sie nun in der Mitte auf „Datenschutz & Personalisierung" – alternativ in der linken Navigationsleiste auf „Daten & Personalisierung" und danach auf „Personalisierte Werbung" (nach etwas Scrollen in der Mitte des Browserfensters). Anschließend klicken Sie auf „Zu den Einstellungen für Werbung". Bei „Personalisierte Werbung" klicken Sie den Schiebregler neben „Personalisierte Werbung ist aktiviert" an, dann bestätigen Sie mit „Deaktivieren" und „OK".

PERSONALISIERTE WERBUNG MIT GOOGLE VERMEIDEN



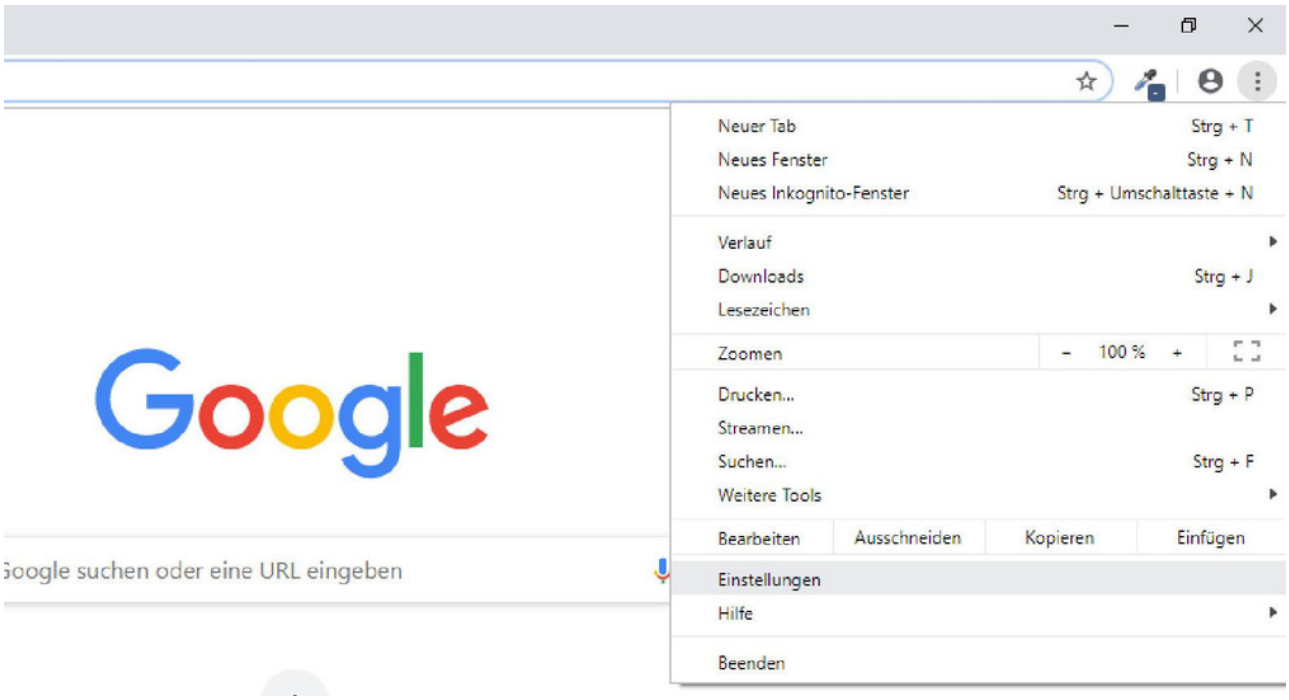
3. Browserdaten, Seitenaufrufe und Cookies löschen

Prüfen Sie die Grundeinstellungen und erweiterten Einstellungen Ihres Browsers, z.B. unter „Einstellungen-Verlauf" „Einstellungen-Sicherheit" und „Einstellungen-Datenschutz". Beim Surfen hinterlässt jeder Nutzer Spuren im Netz. Dazu gehören z.B. Browserdaten, Seitenaufrufe und Cookies. Nach jedem Surfen können Nutzerspuren auf Websites im Browser oder mit Zusatzprogrammen gelöscht werden. Dabei muss jedem Nutzer klar sein, dass damit die Nutzerspuren nur auf dem Smartphone, Tablet oder Desktop-PC gelöscht werden. Der jeweilige Seitenanbieter kann je nach eingesetzter Technik dennoch Informationen über das Nutzerverhalten gesammelt haben und auswerten. Seit 2018 ist das Setzen von Cookies, die Nutzerdaten verwerten, nur noch mit der Einwilligung des Nutzers stattfinden. Die meisten Nutzer sind technisch nicht sehr affin und bestätigen

das mittlerweile gängige Cookie-Banner einfach mit „Ok“. In der Datenschutzerklärung der Website hat der jeweilige Anbieter auf dieses Vorgehen hinzuweisen und den Nutzer über seine Rechte aufzuklären. Das Löschen von Cookies erschwert die Auswertungen des Nutzerverhaltens, da die meisten Tracking-Mechanismen auf dem Setzen von Cookies in den Browsern der Nutzer basieren.

Allerdings kommen zunehmend neue Technologien wie z.B. das sogenannte „Fingerprinting“ zum Einsatz, die dennoch eine Auswertung des Nutzers ermöglichen.

GRUNDEINSTELLUNG "CHROME"



4. Programme nutzen, die die Suchmaschinen und Websites daran hindern, Daten zu sammeln

Es gibt mehrere Möglichkeiten, sich gegen die Daten-Sammelwut von Websites, E-Mail- und Messenger-Diensten, Suchmaschinen und personalisierte Werbung zur Wehr zu setzen. Ein erster, sehr einfacher Schritt: Nutzen Sie die Funktion „Privates Surfen“, wenn Sie sich auf Suchmaschinen bewegen. Auf diese Weise können Websites zumindest keine Cookies mehr setzen und somit Ihr Verhalten nicht vollständig erfassen. Vermeiden Sie auch die Möglichkeit zur automatischen Ausfüllung von Formularfeldern „Auto-Fill“. Wenn Sie das automatische Ausfüllen nicht unterbinden, kann es sein, dass Ihre Angaben (z.B. Name, Telefonnummern, E-Mail-Adressen, Anschriften automatisch in die Felder übernommen werden auch auf Seiten, auf denen Sie das gar nicht beabsichtigen.

Allerdings geht es auch etwas umfassender und komfortabler. Etwa mit dem „Präferenzmanagement-Tool“ von der European Interactive Digital Advertising Alliance: Darüber lässt sich personalisierte Werbung von unterschiedlichen Firmen per Klick deaktivieren.

Eine weitere Möglichkeit sind Werbeblocker, die verhindern können, dass das das Verhalten eines Nutzers über mehrere Seiten hinweg verfolgt wird („tracken"). Allerdings gibt es zunehmend werbefinanzierte Websites, die erst nach Deaktivierung des Werbeblockers angesehen werden können oder es werden neuere Technologien eingesetzt, die Nutzer unbemerkt „verfolgen". Dann greifen Lösungen wie Privacy Badger oder uBlock Origin. Beide sind kleine Erweiterungen für oben genannte Browser. Anhand von Filterlisten und indem sie das Verhalten von Tracking-Cookies beobachten, schließen sie bestimmte Inhalte heraus, die sich nicht an die Regeln des Browsers halten.

5. Betriebssystem und Programme auf dem aktuellen Stand halten

Der Nutzer ist heute oft auf verschiedenen mobilen Endgeräten unterwegs und nutzt auch noch festinstallierte Desktop-PC. Statistiken zeigen, dass auf Smartphones z.B. noch verbreitet veraltete Android-Versionen und auf PCs noch alte Windows-Versionen im Einsatz sind. Unter Windows surften Mitte 2019 noch ein Drittel unter Windows 7 und unter auf Smartphones sind noch die Hälfte veraltete Android-Versionen (Versionen älter als 8.0) unter im Einsatz. Wichtig ist auch, nicht mit Administratorrechten im Internet zu surfen, um die möglichen Auswirkungen von Schadsoftware auf das Betriebssystem zu reduzieren – hier finden Sie dazu eine Anleitung. Aus Gründen der IT-Sicherheit ist es unbedingt ratsam, aktuelle Betriebssysteme und Internet-Browser und Programme zu nutzen, die laufend aktualisiert werden und bei erkannten Sicherheitslücken auf dem aktuellen Stand gehalten werden. Ansonsten kann beim Surfen Schadsoftware auf Smartphone, Tablet und Rechner gelangen, die Nutzerdaten abgreift und weiteren Schaden anrichten kann bis zur totalen Blockade des Geräts.

6. Mit verschiedenen Geräten surfen

Wer unterwegs mit dem Smartphone oder Tablet surft und zuhause den Desktop-PCs nutzt, erschwert das Verfolgen des Nutzers im Netz. Allerdings wurde auch diese „Schwachstelle" von E-Commerce-Anbietern erkannt, so dass zunehmend Methoden des Geräte-unabhängigen „Trackings" entwickelt und zum Einsatz kommen („Cross Device-Tracking"). Um individuelle Nutzer auch auf unterschiedlichen Geräten zu erkennen und ihre Daten in einem Profil zusammenzufassen, werden Methoden wie „Deterministic" oder „Probabilistic Matching" eingesetzt. Diese beiden Methoden werden dazu genutzt, Daten zuzuordnen und Cross-Device-Identitäten Ihrer Nutzer zu erstellen

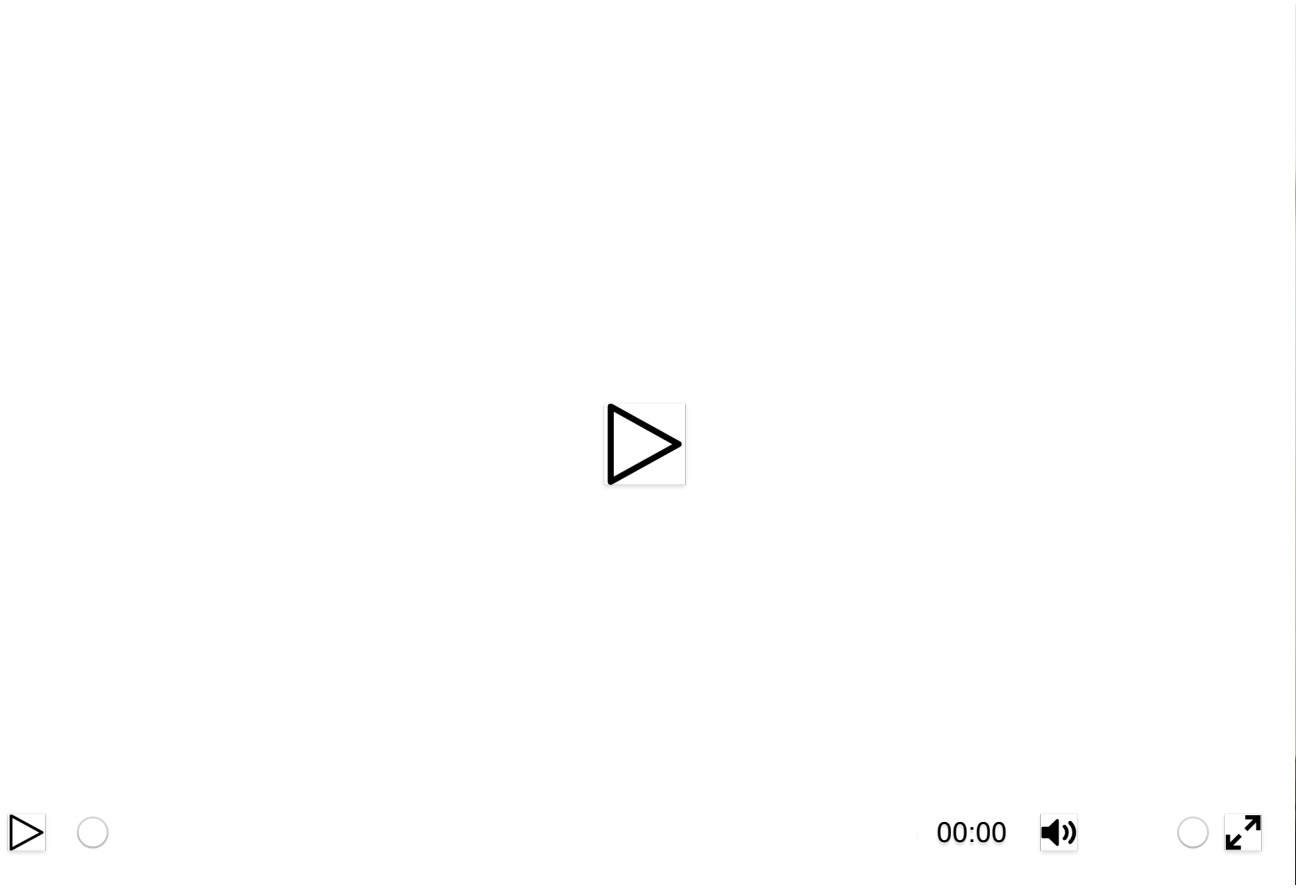
7. Datenauskunft anfordern

Nach europäischem und deutschem Datenschutzrecht sind datenverarbeitende Stellen verpflichtet, allen Nutzerinnen und Nutzer auf Anfrage Auskunft über die über sie gespeicherten Daten zu gewähren. Der Verbraucherzentrale Bundesverband (VZBV) bietet für das Auskunftsersuchen ein praktisches Musterschreiben an, das man leicht anpassen und versenden kann – mehr Informationen hierzu finden Sie hier. Es kann durchaus kurz und formlos gehalten werden. Ggf. lassen sich dann Daten löschen.

ZUSATZ-TIPP: Sie können versuchen, auf Ihr Profil Einfluss zu nehmen, indem sie es mit falschen Daten füttern. So können Sie falsche Kaufabsichten streuen oder vorgebliches Interesse an für Sie abwegigen Themen vortäuschen. Auf diese Weise wird das Profil, dass Algorithmen durch Vergleichskriterien von Ihnen bilden, unbrauchbar.

Das sagen die Experten

Prof. Dr. Stefan Funke zum Thema Social Media



European Interactive Digital Advertising Alliance

Website des Werbeblockers „Privacy Badger“ (Englisch)

Download des Werbeblockers „uBlock Origin“ bei Heise

Die Website www.klicksafe.de ist Bestandteil der Initiative klicksafe im CEF (Connecting Europe Facility) Telecom Programm der Europäischen Union für mehr Sicherheit im Internet. In Deutschland ist die Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz gemeinsam mit der Landesanstalt für Medien NRW mit der Umsetzung beauftragt.

Leitfaden zur Einstellung der Administratorenrechte auf Windows-Rechnern

Informationen zur Datenauskunft und zur Nutzung des „Rechts auf Vergessen werden“

Link dieser Seite:

https://mlr.baden-wuerttemberg.de/de/unsere-themen/verbraucherschutz/algorithmen/suchen-und-finden