Datenspuren im Internet vermeiden

Mittwoch, 22 Mai 2019

https://www.datenschutz.de/datenspuren-im-internet-vermeiden/

Das Internet bietet eine Vielzahl von Diensten, deren Nutzung Datenspuren hinterlässt. Oft werden diese gespeichert, ausgewertet und zu **Nutzungs-, Kauf- oder Bewegungsprofilen** verdichtet. Der Grund hierfür ist unter anderem, dass Werbung auf Internetseiten und in Webdiensten das zentrale Finanzierungs- oder Geschäftsmodell vieler Anbieter darstellt. Je genauer diese auf die potenziellen Kunden abgestimmt ist, das heißt, je mehr man über die Kunden weiß, desto mehr lässt sich damit verdienen. Untersuchungen zeigen, dass sich mit **verhaltensbasierter Werbung** mehr als doppelt so viel erlösen lässt wie mit pauschaler Werbung.

Vor diesem Hintergrund ist nicht verwunderlich, dass Interessen, Neigungen und Konsumgewohnheiten der Nutzer, ihr soziales Umfeld und deren Aktivitäten im Netz auf das Interesse der Werbewirtschaft stoßen. Besonders wichtig sind dabei **Soziale Netzwerke und standortbezogene Dienste**. Aber auch außerhalb von Sozialen Netzwerke blickt einem die Werbewirtschaft in Form von **Cookies, Social-Media-Plugins oder Zählpixeln** über die Schulter.

Die IP-Adresse: Wofür wird sie gebraucht und was verrät sie?

Die **Internet Protocol-Adresse, kurz IP-Adresse**, wird bei jedem Klick auf einer Internetseite mit übertragen und liefert die ersten Informationen. Oft lässt sie sich dem Wohnort oder der Region zuordnen, aus der ein Nutzer kommt.

Die **IP-Adresse wird benötigt, um Datenpakete im Internet zuzustellen** und kann daher nicht vollständig unterdrückt werden. Sie wird den Nutzern von ihrem jeweiligen Internet-Provider zugewiesen und stellt nach Auffassung der Datenschutzbeauftragten ein grundsätzlich personenbeziehbares Datum dar. Dies ist deshalb der Fall, weil nicht nur der Provider in der Lage ist, die IP-Adresse einem Nutzer zuzuordnen, sondern auch jeder Anbieter einer Webseite, auf der sich der Nutzer registriert oder anmeldet oder wo er Name oder Adresse hinterlässt. Zwar wird der Personenbezug in vielen Fällen durch eine dynamische, das heißt wechselnde Vergabe von IP-Adressen relativiert. Mit Vergabe der künftigen IPv6-Adressen entfällt jedoch diese technische Notwendigkeit und ein einmal hergestellter Personenbezug kann dauerhaft bestehen bleiben.

Was sind Cookies und warum können sie problematisch sein?

Cookies sind Textdateien, die eine Webseite auf dem Computer, Tablet oder Smartphone des Nutzers ablegt, um darin Daten zu verschiedenen Zwecken zu speichern. In Cookies wird unter anderem gespeichert, welche Produkte sich beim Online-Kauf im Warenkorb befinden. Auch persönliche Einstellungen werden darin gespeichert. Cookies können von der Webseite stammen, die Nutzer besuchen, oder von Werbeanbietern, die auf der besuchten Seite Werbung schalten. Dies sind sogenannte **Drittanbieter-Cookies**.

Problematisch sind alle Cookies, die eine **eindeutige Kennzeichnung** – die sogenannte ID – enthalten, anhand derer ein Nutzer für die Dauer der Gültigkeit des Cookies wiederzuerkennen ist und deren Gültigkeit über das Ende der Sitzung hinaus reicht. Solche Cookies werden genutzt, um das Nutzerverhalten auf einer Webseite zu erfassen, also zum Beispiel, was ein Nutzer sich auf der Webseite anschaut, wie lange er dort bleibt, was er anklickt und wie oft, ob er die Seite erstmals besucht oder ob er häufiger vorbeischaut. Im Fall von Drittanbieter-Cookies funktioniert dies oft auch über verschiedene Webseiten hinweg. Der Weg eines Nutzers durch das Internet wird also erkennbar. All diese Informationen werden unter der **Cookie-ID** des Nutzers gespeichert.

Unkritisch sind dagegen **Session-Cookies** (oder „Sitzungs"-Cookies), die nur für die Dauer Ihrer Browsersitzung gelten. Sie werden beim Schließen des Browsers gelöscht.

In dem Informationstext „Datenspuren vermeiden" informiert der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz darüber, wie Internetnutzer in ihren Browsern festlegen können, ob sie Cookies verwenden wollen und ab wann diese Daten gegebenenfalls durch den Browser gelöscht werden.

Zählpixel und Web-Bugs

„Zählpixel" oder „Web-Bugs" sind meist **unsichtbare Grafiken, die einen Pixel groß sind** und beim Aufruf einer Webseite geladen werden. Sie stammen wie Drittanbieter-Cookies nicht von der aufgerufenen Webseite, sondern von Werbeplattformen oder Analyse-Diensten, die auf diese Weise den Weg des Nutzers durch das Internet erfassen. Zählpixel können mit Browser-Erweiterungen umgangen werden. Die Weiterleitung der Daten wird durch die Erweiterungen schlicht unterbunden.

Manche Webseiten unterstützen die **„Do-Not-Track"-Initiative**, bei der dem Wunsch der Nutzer entsprochen wird, mit ihrem Surfverhalten nicht erfasst zu werden. In den Browsereinstellungen kann der Nutzer die hierfür erforderliche „Do-Not-Track"-Funktion aktivieren, woraufhin der Browser der Webseite signalisiert, dass der Nutzer nicht verfolgt werden möchte.

Social-Media-Plugins

Wenn Social-Media-Plugins in einer Weise verwendet werden, dass **personenbezogene Daten bereits beim Laden der Webseite Dritten zur Verfügung gestellt** und die Daten von den Dritten zu eigenen Zwecken genutzt werden, verstößt dies gegen die DS-GVO. Diese Datenverarbeitungen sind regelmäßig nicht von Art. 6 Abs. 1 Buchst. f) gedeckt, sodass es einer Einwilligung durch die Nutzer bedarf. Dies bedeutet für die Webseiten- und Blogbetreiber, dass die Plugins technisch so eingebunden werden, dass Datenübermittlungen erst erfolgen, wenn die Nutzer auf die entsprechenden Buttons drücken und eine den Anforderungen der DS-GVO entsprechende Einwilligung erteilt haben. Dies bedeutet, dass sie ausreichend informiert werden und durch eine eindeutige Handlung (zum Beispiel per Häkchen) zustimmen müssen.

Browserdaten

Browser ist nicht gleich **Browser**. Diese Programme zum Surfen im Internet unterscheiden sich in Version, Konfiguration, Spracheinstellung, Bildschirmauflösung und vielem mehr. Durch diese

individuellen Einstellungen entsteht eine Art **digitaler Fingerabdruck**, der sie für Webseitenbetreiber wiedererkennbar macht (auch Device-Fingerprinting). Der Browser verrät zudem über den sogenannten **Referrer**, auf welcher Internetseite der Nutzer zuvor gewesen ist. Nicht alle Browser erlauben es, den Referrer zu deaktivieren.

Viele Browser sind nach der Installation so eingestellt, dass sie die vom Nutzer besuchten Webseiten in einer „Chronik“ speichern. Dieser sogenannte **Browserverlauf** lässt also erkennen, wo man im Internet gewesen ist. Zunächst kann nur der Nutzer, der Zugriff auf die Chronik hat, diesen Verlauf einsehen. Manche Browser bzw. Browserversionen sind jedoch anfällig dafür, dass von außen geprüft werden kann, ob bestimmte Seiten besucht wurden oder nicht. So ist auch von außen erkennbar, wofür sich ein Nutzer interessiert hat.

Suchmaschinen

Jedes Mal, wenn ein Internetnutzer eine Suchmaschine wie **Google, Bing oder Yahoo** nutzt, erzeugt dies eine **Datenspur**. Zwar ist daraus nicht direkt erkennbar, welche Person hinter der Datenspur steht, dies kann sich jedoch schnell ändern. Was Suchmaschinen über ihre Nutzer wissen, lässt sich am Beispiel von Google auch über dessen Dienst „Dashboard“ erkennen. Für jeden Nutzer, der bei Google für einen der zahlreichen Dienste registriert ist, zeigt das Dashboard, wonach über Google gesucht wurde, welche Orte oder Routen auf Google Maps für den Nutzer von Interesse waren, wie sich die Internet-Aktivitäten monatlich, wöchentlich oder täglich verteilen und vieles mehr.

Als Alternative zu Google gibt es datenschutzfreundliche Suchmaschinen, die weniger oder keine Daten speichern, zum Beispiel www.startpage.com (arbeitet mit dem Google-Suchalgorithmus).

Diese Einführung ist auf Basis folgender Texte entstanden:

„Datenspuren vermeiden“ *des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz*

„Hinweise zur Verarbeitung von Nutzungsdaten durch Blogs bzw. Webseiten“ *der Berliner Beauftragten für Datenschutz und Informationsfreiheit*

Für ausführlichere Informationen können Sie unter den folgenden Links recherchieren.

Weiterführende Links zu diesem Thema

Cookies der Datenschutzstelle Fürstentum Lichtenstein

Selbstdatenschutz – Rund um Ihre PC-Nutzung und Sicherheit der Berliner Beauftragten für Datenschutz und Informationsfreiheit

Social Plugins des Bayrischen Landesbeauftragten für den Datenschutz

---

Empfehlungen für die Nutzung von Online- und Social Media-Diensten des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

---

E-Mail Inhalte schützen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

---

Cloud-Speicher sicher nutzen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

---

Spione in der Hosentasche des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

---

„Häufig gestellte Fragen und Probleme beim Versand und Erhalt von E-Mails“ bei dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein

---

„Fragen und Antworten – Telekommunikation“ bei dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

---

„Fragen und Antworten – De-Mail (Anbieter)“ bei dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

---

„Fragen und Antworten – De-Mail (Nutzer)“ bei dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

---

„FAQ zu Cookies und Tracking“ bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg

---

„FAQ Internet“ bei dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

---