

The Cost of Knowledge

Revista de acceso abierto



Bib um 12 - *Special*
Herzlich willkommen!

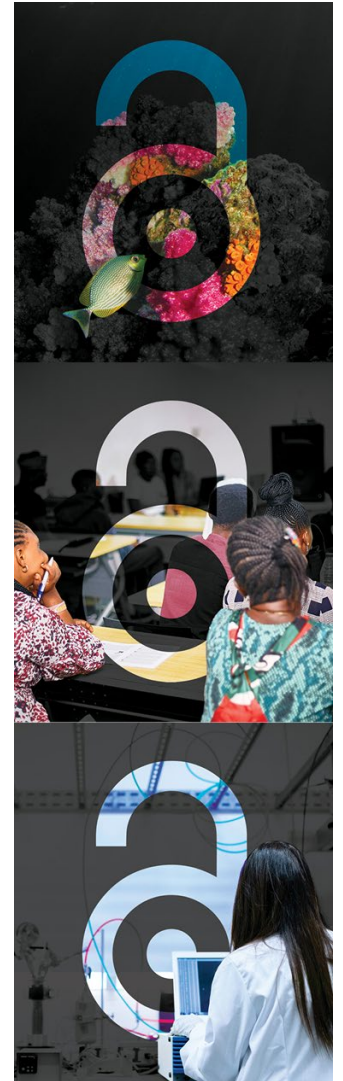
Wissen kostet Daten

Daten-Tracking in der Wissenschaft

Fabian Franke

fabian.franke@uni-bamberg.de

Universitätsbibliothek Bamberg



Datentracking in der Wissenschaft: Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage

Ein Informationspapier des Ausschusses für
Wissenschaftliche Bibliotheken und Informationssysteme
der Deutschen Forschungsgemeinschaft

28. Oktober 2021

<https://www.dfg.de/resource/blob/174922/datentracking-papier-de.pdf>

Seit einiger Zeit verändern die großen wissenschaftlichen Verlage ihr Geschäftsmodell grundlegend mit erheblichen Auswirkungen auf die Wissenschaften: Die Aggregation und die Weiterverwendung bzw. der Weiterverkauf von Nutzerspuren werden relevante Aspekte der Verlagstätigkeit. Verlage verstehen sich jetzt teilweise ausdrücklich als Unternehmen für Informationsanalysen.



<https://www.dfg.de/resource/blob/174922/datentracking-papier-de.pdf>

Das Geschäftsmodell der Verlage wandelt sich damit von Content Providern hin zu einem Data Analytics Business. Dabei werden die Daten von Wissenschaftlerinnen und Wissenschaftlern (das heißt personalisierte Profile, Zugriffs- und Nutzungsdaten, Verweildauern bei Informationsquellen usw.) bei der Nutzung von Informationsdiensten wie z. B. der Literaturrecherche getrackt, das heißt festgehalten und gespeichert.

<https://www.dfg.de/resource/blob/174922/datentracking-papier-de.pdf>

Kontrolle des Wissenschaftsmarkt

Die Big Five – Elsevier, Springer Nature, Wiley, Taylor & Francis und Sage – waren 2022 für 61% der wissenschaftlichen Artikel verantwortlich und vereinigten 50% der Umsätze auf sich, mit Gewinnmargen bis zu 38%.

Crotty, D. (2023). Quantifying Consolidation in the Scholarly Journals Market.

<https://scholarlykitchen.sspnet.org/2023/10/30/quantifying-consolidation-in-the-scholarly-journals-market/>

Tracking als System



RELX | Reed Elsevier ... is a global provider of information-based analytics and decision tools for professional and business customers.



„technology-enabled products, platforms and services



a global company that provides digital education, learning, assessment and certification solutions for various sectors and subjects

Tracking

„the collection of data about an individual’s activity across multiple distinct contexts and the retention, use, or sharing of data derived from that activity outside the context in which it occurred.“

Binns, R. (2022). *Tracking on the Web, Mobile and the Internet-of-Things*.

<https://doi.org/10.48550/ARXIV.2201.10831>

Trackingmethode	Beschreibung	Formen, Beispiele	Anwendung	Konsequenzen
Geofencing + IP-Targeting	Ineinandergreifende Verfahren der Lokalisierung von Geräten bzw. Personen durch das Hochschulnetz und darin durch mobile Geräte ²²	Geofencing kann zum Tracken von mobilen Geräten verwendet werden, durch GPS, Bluetooth, WLAN und auch Radiowellen (Bashyakarla, o. J., S. 57), IP-Targeting betrifft auch physische Adressen	Lokalisierung von Institutionen und Personen, Überwachung	„gezielte, standortbezogene Übermittlung von Inhalten über die IP-Adresse [...] kann nicht nur bestimmte Geräte, sondern auch hinter den IP-Adressen stehende Haushalte, Betriebe, Institutionen und deren Subnetze wie auch Fachbereiche und Bibliotheken adressieren.“ (Freiberg, 2022, S. 98)
Authentifizierungsform	Anbieter stipulieren die Nutzung bestimmter Authentifizierungsmethoden, die eine anonymisierte Nutzung ihrer Angebote, z.B. nur durch die Authentifizierung als Institutionsmitglied, verunmöglichen ²³	Domainübergreifende Authentifizierungsverfahren: Single-Sign-On, RA21 zu SeamlessAccess.org zu GetFTR	Kontrolle über Nutzer:innen von Bibliotheksdiensten bzw. Hochschulnetzen	Online-Verhalten von eingeloggtten Nutzenden wird beobachtet, sie werden auf Verlagsplattformen umgeleitet; „The architecture of GetFTR is designed to take place behind the scenes, with no ability for libraries or other users to opt out“ (SPARC, 2021, S. 8)
Port Scanning	Identifikation durch Ausnutzung von Sicherheitslücken in Browsern/Servern	Suche nach Schwachstellen in Endgeräten oder Netzwerken	Form der Individuierung, Hacking	„Schon die Suche nach offenen Ports auf fremden Rechnern und/oder Netzwerken [...] ist nach deutschem Verständnis am Rand der Legalität, da sie als Vorstufe von entsprechend sanktionierten Tatbeständen (§§ 202c, 303b StGB) gewertet werden kann.“ (DFG AWBI, 2021, S. 11)
Device/Browser- & Personen-Fingerprinting	Individuierung von Geräten sowie geräteübergreifend von Personen über die Erstellung von Profilen ihrer Geräte bzw. biometrischer Merkmale der Gerätebedienung	Double Click, BehavioSec	Identifizierung von Personen durch behavioral-biometrische Profilbildung	Erfassung auch derjenigen, die Maßnahmen gegen Tracking ergreifen bzw. durch institutionelle Sicherheitsmaßnahmen geschützt sind; geräteübergreifende Profilbildung
History-Sniffing	Zugriff auf die Verbindungshistorie im Browser, um das Surfverhalten zu verfolgen (SPARC, 2023, Appendix C-3 und C-4)	über JavaScript	Spionage und Überwachung	„Der Javascript-Code der Third Parties [...] kann [...] auslesen, mit welchem Text der Nutzer sich beschäftigt, zu welchem er als nächstes weiterbrows und welche Suchworte er auf der Plattform eingibt.“ (DFG AWBI, 2021, S. 10)
Cookies	Code auf Geräten der Endnutzer:innen, der von first und third party gesetzt wird. Reicht von einfacher Analyse bis zu sitzungsübergreifender Verfolgung und praktisch nicht entfernbaren Versionen	first / third party cookie, evercookie (QuantCast, KISSmetrics)	Erstellung und Verwertung von Profilen, Analytics als Überwachung von Aktivitäten	Profilerstellung, cross-site-tracking Überwachung digitaler und analoger Aktivitäten
Tracking-Pixel (alternative Bezeichnungen: Zählpixel / Web-Bugs, Web-Beacons, Web-Wanzen)	Elemente, (ähnlich wie Cookies) durch third parties auf Websites platziert, um verschiedene Informationen über das Endgerät zu übermitteln, z.B. IP-Adresse, Betriebssystem, Browser-Konfigurationen. In E-Mails platziert informieren sie third parties darüber, ob eine E-Mail geöffnet wurde	Transparente Ein-Pixel-Bilder, für das Auge unsichtbar, Elsevier cookie notice	Eindeutige Individuierung, Analytics als Überwachung von Aktivitäten, Profilerstellung	Übermitteln an Drittparteien (Google, Adobe, Cloudflare, New Relic) Daten, die zur Identifizierung von Personen führen können (vgl. SPARC, 2023, S. 24); „Der einzige Zweck von Zählpixeln besteht darin, dass der Browser des Nutzers Kontakt mit dem Tracker aufnimmt.“ (Schneider et al., 2014, S. 41)

Deal-Verträge



Elsevier will not generate, track, record, store, share, transfer, and/or sell personal data of Authorized Users without the consent of the respective Authorized User ..., unless the processing is necessary for ...



Science Tracking: Publisher is obligated not to track, record, store share, transfer and/or sell usage data or personal data of users accessing content under the Agreement, unless absolutely necessary ...



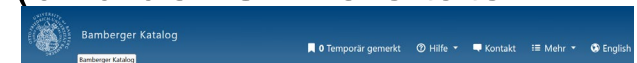
Wiley will not track, record, store, share, transfer and/or seil usage or personal data of Authorized Users (Science Tracking) without the consent of the Authorized User, unless the processing is necessary ...

Wo gibt es kein Daten-Tracking?



- ~~Auf allen Plattformen, die von Bibliotheken und Fachgesellschaften verantwortet werden.~~

- Im Bibliothekskatalog der UB Bamberg (und der Universitäts- und Hochschulbibliotheken in Bayern)



- Im Forschungsinformationssystem der Universität Bamberg



- In der University of Bamberg Press



Der AWBI möchte mit diesem Informationspapier dazu anregen, einen breiten Diskurs in der Wissenschaft sowohl auf Ebene der wissenschaftlichen Entscheidungsträgerinnen und -träger als auch unter Wissenschaftlerinnen und Wissenschaftlern sowie in Einrichtungen der Informationsinfrastruktur zu führen, um die Praxis des Trackings, dessen Rechtmäßigkeit, Maßnahmen zur Einhaltung des Datenschutzes und Konsequenzen der Aggregation von Nutzungsdaten zu reflektieren und geeignete Maßnahmen zu ergreifen.

<https://www.dfg.de/resource/blob/174922/datentracking-papier-de.pdf>

Die Erhebung von Daten über die Wissenschaft und über wissenschaftliche Aktivitäten kann sinnvoll sein, sofern sie transparenten und klaren Vorgaben folgt, Risiken für einzelne Wissenschaftlerinnen und Wissenschaftler minimiert werden sowie eine Nutzung solcher Daten durch, wenn nicht eine Hoheit über solche Daten bei wissenschaftlichen Organisationen gewährleistet werden kann.

<https://www.dfg.de/resource/blob/174922/datentracking-papier-de.pdf>

Lösungsansätze?



There are no free lunches (and no quick fixes) (Siems, 2022)

<https://stoptrackingscience.eu/>

„Gestaltung des digitalen Raumes als Daueraufgabe von Wissenschaftseinrichtungen“ (Wissenschaftsrat, 2023)

- Ausbau öffentlich geförderter digitaler Infrastrukturen und Plattformen
- transparente Open-Source-Lösungen
- dauerhafte Förderung von Diamond Open Access.

Literaturvorschläge

DFG: Datentracking in der Wissenschaft. Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage. Bonn 2021.
<https://www.dfg.de/resource/blob/174922/datentracking-papier-de.pdf>

Fadeeva, Yuliya. (2026). Science Tracking über Transformationsverträge und Wissenschaftsplattformen. Vom Beifang zum Hauptziel. In: kommunikation@gesellschaft, 26(1).
<https://doi.org/10.15460/kommges.2025.26.1.1643>

Siems, Renke: Das Lesen der Anderen. Die Auswirkungen von User Tracking auf Bibliotheken. In: o-bib 9 (1), 2022. <https://doi.org/10.5282/o-bib/5797>.

Wissenschaftsrat. Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum. 2023. <https://doi.org/10.57674/M6PK-DT95>

The Cost of Knowledge

**Dienstag, 20.10, 12 Uhr: Wer soll das bezahlen? –
Fördermöglichkeiten der UB für Open Access**

**Mittwoch, 21.10., 12 Uhr: The cost of knowledge –
Wer bezahlt eigentlich für Wissen?**

**Freitag, 23.10, 12 Uhr: Die Open Science Policy
der Universität Bamberg**

<https://www.uni-bamberg.de/ub/kurse-tutorials/bib-um-12/>