Gehackte Forschung

Wissenschaftlertracking als Risiko für die Datensicherheit

| ROLF SCHWARTMANN | KRISTIN BENEDIKT | **Die digitalen Produkte von Wissenschaftsverlagen verfolgen jede Aktion ihrer Nutzer. Diese Verhaltensanalysen sind für Firmen und Hacker gleichermaßen wertvoll. Was mit den von ihnen generierten Datenspuren passiert, bleibt Forschenden aber oft unklar. Wie juristisch wasserfest ist das Geschäft mit den Daten? Was gilt für den Datenschutz und wem obliegt die Verantwortung für die Sicherheit von Forschenden und ihren Daten?**

Wissenschaftsverlage vertreiben nicht nur wissenschaftliche Publikationen, sondern sie mausern sich in der Digitalisierung zu Datenverwaltern. Sie sitzen an der Quelle des Fortschritts und ihr Geschäftsgegenstand sind Forschungsdaten, die sie zunehmend im Rahmen neuer Geschäftsmodelle auswerten. Geschäfte machen sie nicht mehr nur mit Büchern, sondern mit Recherchedatenbanken und Wissenschaftsdatenanalysen. Sie bieten digitale All-In-One-Produkte an und verwalten, teilen, analysieren und verwerten Literaturquellen und Forschungsdaten in unterschiedlicher Ausformung. Die Reichweite von Fachpublikationen ist weltweit permanent anhand von Klicks, Downloads, Zitaten und Verbreitungsgeschwindigkeit messbar. Die Forschungsleistung von Einzelnen und gesamten Forschungseinrichtungen kann so anhand der Kriterien von Verlagen verglichen werden und in ihrer Relevanz gesteuert werden.

Die Forschung unterwirft sich auf diese Weise den Gesetzen der Onlinewelt, wo Programmierer von Algorithmen weit mehr Einfluss auf die Wahrnehmung eines Forschungsergebnisses haben als dessen Qualität. Wer mehr Klicks generiert, wird häufiger gesehen, häufiger zitiert und erscheint leistungsfähiger. Diese Indikatoren spielen nicht nur bei der Vergabe von Drittmitteln eine entscheidende Rolle. Die Mechanismen des Wettbewerbs um Klicks beeinträchtigen im Zusammenspiel mit der Datensammelei der Wissenschaftsverlage auch die Forschungsfreiheit. Das ist ein nennenswertes Problem, wie zuletzt die Deutsche Forschungsgemeinschaft (DFG) in ihrem Informationspapier „Datentracking in der Wissenschaft: Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage“ resümiert hat.

Transparenz ist notwendig

Datenschutzrechtlich kommt es bei diesen Geschäftsmodellen vor allem auf Transparenz an, die Forschende und Wissenschaftseinrichtungen in den Stand versetzt, die Zusammenhänge der Auswertung ihrer Forschungsdaten zu begreifen, um sich gegenüber Verlagen bewusst dafür oder dagegen entscheiden zu können. Wenig thematisiert ist bisher, das ernst zu nehmende Sicherheitsrisiko beim Wissenschaftlertracking. Um das Nutzungsverhalten der Forschenden zu erfassen, personalisierte Dienste anzubieten und das verlagseigene Angebot weiterzuentwickeln und zu optimieren, kommen Tracking-Technologien zum Einsatz. Diese haben sich im Bereich der Online-Werbung auf Social Media Plattformen, auf Streamingportalen und werbefinanzierten Websites von Nachrichtendiensten bewährt. Dabei kommt nicht nur verlagseigene Software zum Einsatz, um das Nutzerverhalten zu erfassen. Es werden ebenso Tracking-Tools von Drittanbietern wie zum Beispiel Google, Facebook, Oracle und Adobe verwendet. Die Wissenschaftsverlage rechtfertigen die Nutzung dieser Tracking Tools u.a. damit, potenzielle Bedrohungen zu erkennen, Betrug zu verhindern und unbefugten Zugriff auf geschützte Inhalte zu blockieren. Es sollen Schattenbibliotheken und damit einhergehend Urheberrechtsverletzungen verhindert werden. Das sind legitime Zwecke, doch wer hochsensible Daten über Forschende erhebt, der unterliegt einer besonderen Verantwortung. Wissenschaftsverlage sind als datenschutzrechtlich Verantwortliche verpflichtet, eine Vielzahl von technischen und organisatorischen Maßnahmen zu ergreifen, um die Daten ihrer Nutzer zu schützen. Dazu gehört es, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen, denn Forschungsdaten wecken nicht nur das Interesse von Wissenschaftsverlagen, sondern auch von Cyber-Angreifern.

Das besondere Sicherheitsrisiko entsteht dadurch, dass bei der Einbindung

AUTOREN

Foto: TH-Köln/Schmülgen

Professor Dr. **Rolf Schwartmann** leitet die Forschungsstelle für Medienrecht an der TH Köln und ist Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Kristin Benedikt ist Richterin und Datenschutzbeauftragte am Verwaltungsgericht Regensburg.

von Drittinhalten eine unmittelbare Datenverbindung zwischen dem Endgerät der Nutzer, sprich der Forschenden und den Servern des eingebundenen Dienstes, etwa Facebook oder Adobe, entsteht. Jede Kommunikation zu einem Server ist risikobehaftet, da über den Datenaustausch nicht nur erforderliche Nutzungsdaten und Inhalte ausgetauscht werden, sondern gegebenenfalls auch Schadsoftware. Dabei können schädliche Skripte oder andere Programme ausgeführt werden, die das Endgerät der Forschenden mit Viren oder Trojanern infizieren. Sicherheitslücken, die unter Cyber-Kriminellen auf frei zugänglichen Plattformen ausgetauscht werden, können ausgenutzt werden, um z.B. Verschlüsselungstrojaner zu platzieren. Die Folgen einer solchen Datenschutzverletzung sind weitreichend, wie erst kürzlich das Beispiel der TU Berlin zeigte. Dort waren Ende April 2021 Windows-Teilbereiche der Computersysteme „massiven Angriffen“ ausgesetzt. Ungeahnte Ausmaße kann ein solcher Cyber-Vorfall bekommen, wenn es sich bei den Forschungseinrichtungen zugleich um Universitätskliniken oder überhaupt um kritische Infrastrukturen handelt und deren Systeme kompromittiert werden.

> »Jede Kommunikation zu einem Server ist risikobehaftet.«

Pflicht zur Datensicherheit

In solchen Fällen geht es nicht „nur“ um den Datenschutz, sondern die höchsten Güter: Leben und körperliche Unversehrtheit. Für den Fall, dass es zu einem Cyber-Vorfall kommt, bestimmen die Datenschutzgesetze, dass die Wissenschaftsverlage als Diensteanbieter die Verfügbarkeit und den Zugang zu den Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen haben. Die gleiche Verpflichtung betrifft übrigens auch Forschungseinrichtungen, die die digitalen Bibliotheken und Dienstleistungen der Wissenschaftsverlage ihren Forschenden zur Verfügung stellen. Doch wie stellt man verschlüsselte Forschungsdaten rasch wieder her? Die Forderung der Angreifer ist klar. Lösegeld in Bitcoin bezahlen! Ihr sollte man auf keinen Fall nachkommen. Denn niemand garantiert, dass die Daten entschlüsselt werden können. Außerdem sind zahlende „Opfer“ das perfekte Ziel für einen erneuten Angriff.

Wenn die Daten verschlüsselt bleiben, sind sie womöglich verloren. Wer kommt für den Schaden auf und wie viel sind Forschungsdaten eigentlich wert? Auf diese Fragen sollten Hochschulen, die digitale Produkte einsetzen, und insbesondere auch Wissenschaftsverlage eine Antwort haben, und zwar bevor die Tracking Tools zum Einsatz kommen. Antworten finden Sie, indem sie eine weitere Pflicht zur Datensicherheit erfüllen und eine Datenschutzfolgenabschätzung vornehmen. Diese ist nach der Datenschutz-Grundverordnung immer dann durchzuführen, wenn neue Technologien zum Einsatz kommen und aufgrund der Art, des Umfangs oder der Umstände ein hohes Risiko besteht. Diese Voraussetzungen liegen bei Tracking-Tools im Forschungsbereich vor. Außerdem besteht die Pflicht, Cyber-Angriffe bei der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden zu melden. Ein Verstoß gegen die Meldepflicht kann zu einem Bußgeld führen. Forschungseinrichtungen, die zugleich öffentliche Stellen sind, haben zwar kein Bußgeld zu befürchten, wohl aber schlimme Imageverluste. Anderes gilt hingegen bei privaten Forschungseinrichtungen und den Wissenschaftsverlagen als Betreiber der Dienste, wo Bußgelder fällig werden können. Wenn Verlage, wie kürzlich Elsevier dem Vorwurf der Deutschen Forschungsgemeinschaft Tracking-Tools einzusetzen, damit begegnen, dass Tracking im weitesten Sinne der Datensicherheit dient, haben sie hoffentlich berücksichtigt, dass der „Angreifer“ nicht nur der Forschende ist, der die Pay-Wall umgeht, sondern auch jeder Hacker. Ihn hat das Datenschutzrecht unabhängig vom Urheberrecht im Auge und seine Abwehr muss mit zunehmender Digitalisierung in den Fokus von Verlagen und Forschungseinrichtungen rücken.

> »Wenn die Daten verschlüsselt bleiben, sind sie womöglich verloren.«

KLEINE FÄCHERKUNDE

Foto: Universität Würzburg

Georg Nagel ist Professor am Physiologischen Institut der Universität Würzburg und forscht in der Abteilung Neurophysiologie zu Optogenetik.

Was erforschen Sie?

Seit über 20 Jahren erforsche ich mit meiner Gruppe hauptsächlich Photorezeptoren (Licht-sensitive Proteine) aus Mikroben und suche mit Kooperationspartnern nach Anwendungen **(Optogenetik)**. *Ausgebildet zum Elektrophysiologen ging es ursprünglich um den Transport von Ionen („Salzpartikeln“) über die Zellmembran, denn ein veränderter Ionentransport kann z.B. Krankheiten von Herz, Nerven oder Verdauung bewirken.*

Was fasziniert Sie daran?

Mikroben haben mit uns Menschen den Aufbau der Zelle gemeinsam, haben aber oft ganz andere Problem-Lösungen gefunden. Der Erfindungsreichtum der Natur scheint dabei fast unendlich zu sein. Faszinierend ist, dass wir heutzutage Proteine aus Mikroben in Tiere oder Pflanzen bringen können und damit ganz neue Anwendungen erschließen.

Für wen ist das wichtig?

Ob unsere Forschungserkenntnisse wichtig sind, stellt sich immer erst nach einiger Zeit heraus, mal nach kurzer mal nach längerer. Channelrhodopsin, ein Licht-sensitiver Ionenkanal aus einer einzelligen Grünalge, wurde erstmals 2002 von uns kloniert und charakterisiert. Schon nach wenigen Jahren wurde es erfolgreich in der Neuro-Grundlagenforschung eingesetzt, dann Optogenetik genannt. 2021, fast 20 Jahre später, wurde der erste Patient beschrieben, dessen Blindheit teilweise geheilt wurde, indem ihm ein Channelrhodopsin gentechnisch „eingepflanzt“ wurde. Auf die Optogenetik trifft man zur Zeit hauptsächlich in den Neurowissenschaften, sie ist aber nicht darauf begrenzt.