idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
Cornelia Reitz
11/20/2023
http://idw-online.de/en/news824328

Research results, Scientific Publications
Information technology, Law
transregional, national

Studie: Fehlende Rechtssicherheit für Big Data und KI

Rechtlicher Rahmen reicht aktuell nicht aus – Problem zum Beispiel bei der Anonymisierung personenbezogener Daten Wie können Big-Data- und KI-Anwendungen gewinnbringend genutzt werden, ohne Datenschutz und IT-Sicherheit zu verletzen? Mit dieser Frage beschäftigt sich eine juristische Studie des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE. Die Autorinnen und Autoren der Studie „Systematic Privacy in real-life Data Processing Systems“ untersuchen geltende Vorschriften aus den Rechtsbereichen Datenschutz, IT-Sicherheitsrecht und Urheberrecht in Bezug auf Big Data.

Dabei betrachten sie auch den Entwurf über eine EU-Verordnung zur Künstliche Intelligenz (KI-VO-E). Ihr Fazit: Der aktuelle Rechtsrahmen reicht für eine sichere Verarbeitung von Big Data nicht aus und sorgt für Verunsicherung bei Bürgerinnen und Bürgern sowie Rechtsunsicherheit bei Unternehmen. Sie fordern einen ganzheitlichen, rechtlich-technischen Rahmen und entwickeln konkrete Lösungsvorschläge sowie Handlungshilfen. Die vollständige Studie kann kostenlos unter https://www.athene-center.de/forschung/leap-studien heruntergeladen werden.

Mit der Digitalisierung von Prozessen in Verwaltung und Wirtschaft fallen riesige Mengen an digitalen Datensätzen aus verschiedenen Quellen und in ganz unterschiedlichen Formaten an (Big Data). Die Verarbeitung dieser großen Datensätze birgt erhebliche Chancen für Wirtschaft und Gesellschaft, beinhaltet aber auch Risiken für Verletzungen des Persönlichkeitsrechts von Bürgerinnen und Bürger. Beispiele gibt es viele: Im Katastrophenschutz lassen sich Personen über Big-Data-Analysen von Handydaten schneller finden und evakuieren. In Schulen lassen sich mittels Big-Data-Analysen Stärken und Schwächen von einzelnen Schülerinnen und Schülern erfassen und daraus individuelle Lernprogramme entwickeln. Ein weiteres Einsatzfeld für die staatliche Nutzung von Big-Data-Analysen ist der Arbeitsmarkt: So werden in Österreich und Polen die Arbeitsmarktchancen arbeitsloser Personen errechnet und kategorisiert.

KI und Big Data

ChatGPT, Midjourney und Co., Anwendungen, die Künstliche Intelligenz nutzen, sind zurzeit in aller Munde. Diese und andere KI-Anwendungen verarbeiten riesige, reale Datenmengen – was viele rechtliche Fragen aufwirft: Dürfen für das Training von KI-Anwendungen beliebige Daten aus dem Internet genutzt werden, welche Schutzrechte greifen hier? Wenn Daten rechtmäßig gewonnen wurden, wem gehören die Ergebnisse der Verarbeitung, also der KI-generierte Daten? Wer haftet im Zweifel für die Ergebnisse? Die Studie untersucht, welche Antworten geltendes Recht (Urheberrecht, Datenschutzrecht, IT-Sicherheitsrecht) liefert, und geht besonders auf die geplante KI-Verordnung der EU (KI-VO-E) ein. Die Autorinnen und Autoren fassen wichtige Bestimmungen zusammen, sehen allerdings aktuell noch viele Herausforderungen für KI-Betreiber, hier sichere vertragliche Regelungen für die Datenverarbeitung zu finden, ohne den eigenen Spielraum zur Verwertung der Ergebnisse zu sehr einzuengen.

Wann sind Daten anonym?

Die Autorinnen und Autoren der Studie sehen ein grundlegendes Problem bei der Anonymisierung von personenbezogenen Daten, um sie zu verarbeiten: Ab wann sind (ehemals) personenbezogene Daten verlässlich und rechtssicher anonymisiert? Hier gibt das geltende Recht (insbesondere die DSGVO) keine abschließende Antwort, was zu Rechtsunsicherheiten für verarbeitende Unternehmen und Einrichtungen führt. Eine mögliche Lösung wäre, einen Grad der Anonymisierung durch ein einheitliches Verfahren zu berechnen und einen Schwellenwert für die legale Nutzung anzusetzen. Dadurch könnten Unternehmen Rechtssicherheit erreichen.

Ganzheitlicher Rechtsrahmen für Big Data

Die jetzige Rechtslage für Big Data lässt viele Fragen offen. Die Studie kommt zu dem Schluss, dass ein ganzheitlicher Ansatz vonnöten ist. Dieser sollte übergreifend verschiedene Rechtsgebiete berücksichtigen, um einerseits Bürgerinnen und Bürger zu schützen, andererseits Unternehmen wie Herstellern Rechtssicherheit zu geben und somit die Nutzung neuer Technologien unter Berücksichtigung von Datenschutz und IT-Sicherheit zu ermöglichen.

Die Studie ist im ATHENE-Projekt „Systematic Privacy in real-life Data Processing Systems“ entstanden. Im Projekt werden die Wissenschaftlerinnen und Wissenschaftler noch weiter zu den aufgeworfenen Fragen forschen und konkrete Vorschläge erarbeiten, mit dem Ziel, die Vorteile von Big Data und KI rechtssicher nutzen zu können, ohne dass dies unangemessene Eingriffe in die Rechte und Freiheiten betroffener Personen mit sich bringt. Die Autorinnen und Autoren sind an vier im Bereich des Digitalisierungsrechts führenden hessischen Lehrstühlen bzw. Forschungseinrichtungen tätig: Gerrit Hornung und Till Schaller, Universität Kassel; Annika Selzer, Sarah Stummer und Jessica Kriegel, Fraunhofer-Institut für Sichere Informationstechnologie SIT; Indra Spiecker gen. Döhmann und Amina Gutjahr, Goethe-Universität Frankfurt sowie Thomas Wilmer, Hochschule Darmstadt (h_da). Alle sind zugleich Angehörige von ATHENE.

Das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE ist das größte Forschungszentrum für IT-Sicherheit und Privatsphärenschutz in Europa. ATHENE ist eine Forschungseinrichtung der Fraunhofer-Gesellschaft mit ihren beiden Instituten Fraunhofer SIT und IGD unter Beteiligung der TU Darmstadt, der Goethe-Universität Frankfurt und der Hochschule Darmstadt.

contact for scientific information:
Dr. Annika Selzer

Original publication:
https://www.athene-center.de/forschung/leap-studien

Die Autorinnen und Autoren der Studie „Systematic Privacy in real-life Data Processing Systems“ untersuchen geltende Vorschriften aus den Rechtsbereichen Datenschutz, IT-Sicherheitsrecht und Urheberrecht in Bezug auf Big Data.
ATHENE