Chancen und Risiken intelligenter Systeme

Bereits vor gut 30 Jahren waren die Themen „Künstliche Intelligenz" (KI) und „Maschinelles Lernen" (ML) schon „Hype" genug, um das „Deutsche Forschungszentrum für Künstliche Intelligenz" (DKFI) zu gründen. Nun erfahren diese Themen mit dem kürzlich verabschiedeten Strategiepapier „Eckpunkte der Bundesregierung für eine Strategie Künstliche Intelligenz" gerade wieder eine Renaissance.

Forscher und Anwender erschließen in diesen Bereichen immer noch „Neuland", sei es bei den entsprechenden rechtlichen Grundlagen, sei es bei den technischen Anwendungen. Und nicht zuletzt sind solche Systeme im Rahmen von „intelligenten" Fahrzeugen auch im Alltag von uns allen angekommen, die Diskussion zu den sich hieraus ergebenden ethischen Problemen sind bereits in vollem Gange. Grund genug also, sich mit den Themen auch einmal aus der speziellen Sicht des Datenschutzes und der Informationssicherheit zu beschäftigen.

Mit den Beiträgen dieses Schwerpunktheftes wollen wir dem Leser dazu eine Einführung in die technischen Hintergründe und mögliche Anwendungsszenarien in den Bereichen der Informationssicherheit und des Datenschutzes geben. Die Autoren zeigen dabei anhand von Praxisbeispielen auf, welche konkreten Problemfelder noch bestehen, diskutieren Sinnhaftigkeit und Machbarkeit der Lösungen und stellen zudem ihre eigenen Lösungsansätze vor.

Im ersten Themenblock betrachten die Autoren zunächst die rechtlichen Aspekte und leiten daraus entsprechende Anforderungen für den Einsatz in der Praxis ab:

- Im Beitrag **Künstliche Intelligenz und internationales Recht: mögliche Entwicklungen und Hindernisse** geht Thomas Burri zunächst der Frage nach, welche Schlussfolgerungen sich aus der Betrachtung des internationalen Rechts ergeben.
- Das Autorenteam rund um Felix Bieker stellt in seinem Beitrag **Verantwortlichkeit und Einsatz von Algorithmen bei öffentlichen Stellen** heraus, dass vor allem die Überprüfbarkeit und Transparenz der Algorithmen wichtige Aspekte sind, um den Anforderungen des Datenschutzes gerecht zu werden.
- Bernhard Waltl und Roland Vogl greifen dies im Beitrag **Increasing Transparency in Algorithmic-Decision-Making with Explainable AI** wieder auf und erläutern, ob und wie Tests und Audits der Algorithmen hier unterstützen können.

Der zweite Themenblock beschäftigt sich mit den technischen Grundlagen und möglichen Anwendungen von ML und KI im Bereich der Informationssicherheit.

- **Maschinelles Lernen und künstliche Intelligenz in der Informationssicherheit** titelt der Beitrag von Thomas Dullien. Er beschreibt die mathematischen Algorithmen, zeigt auf, wo diese ihre Grenzen haben und wie wichtig eine zur jeweiligen Anwendung passende Datenbasis ist.
- Dror-John Röcher diskutiert im Beitrag **Cyber Threat Intelligence 101** mögliche praktische Anwendungen von ML und KI im Bereich der Cyber-Sicherheit und erläutert die Probleme bei der Unterscheidung von Gut und Böse.
- Abschließend widmet sich Thomas Hemker dem Thema **Machen Maschinen die Welt sicherer?** und geht dabei unter anderem der Frage nach, wie auch Angreifer intelligente Algorithmen für sich selbst nutzen können.

Der Aufsatz von Hans-Christian Brockmann mit dem Titel **Effizientes und verantwortungsvolles Datenmanagement in Zeiten der DSGVO** schlägt schließlich eine Brücke zum Themenkomplex der Datenschutz-Grundverordnung. Er erläutert mit optimistischer Herangehensweise, wie das Datenmanagement auf Metadatenebene gelingen kann. Ergänzt wird der Schwerpunkt des Heftes darüber hinaus durch einen Aufsatz **Wissenschaftliche Forschung und Datenschutz** von Christian Geminn, in dem er den möglichen Konflikt zwischen Forschungsfreiheit auf der einen und informationeller Selbstbestimmung auf der anderen Seite beleuchtet.

Zusammen mit dem gesamten Herausgeberteam wünsche ich Ihnen als Gastherausgeber eine informative und spannende Lektüre. Wir hoffen, dass auch diese Ausgabe Ihnen, verehrte Leserinnen und Leser, Impulse für Ihre tägliche Arbeit gibt.

Christoph Wegener