Künstliche Intelligenz datenschutzrechtlich gestalten

Künstliche Intelligenz ist eine (eher forschungspolitische) Sammelbezeichnung für moderne Informationssysteme, die nach der Definition der hochrangigen Expertengruppe der Europäischen Union für Künstliche Intelligenz „ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen". Gemeinsam ist den unterschiedlichen Gruppen von IT-Systemen, dass sie die Strukturierung großer Datenmengen durch Mustererkennung und Modellbildung ermöglichen und aufgrund ihrer Ergebnisse selbsttätig bestimmte Entscheidungen treffen oder Funktionen ausführen können. Ihre Programme sind entweder durch komplexe Algorithmen festgelegt oder lernen selbst durch die betreute Verarbeitung großer Datenmengen. Unter Künstliche Intelligenz werden wichtige Technikentwicklungen gefasst, die für die Digitalisierung aller Wirtschafts-, Verwaltungs- und Gesellschaftsbereiche große Bedeutung haben. Anwendungsbereiche sind zum Beispiel die Gesundheitsversorgung, der Verkehr, der Bankensektor, die automatisierte Fertigung, die Forschung, die Wissensarbeit, unterstütztes Lernen, die öffentliche Verwaltung, die Sicherheitsgewährleistung und Legal Tech. Für alle Anwendungen stellt sich die Frage, wie sie datenschutzgerecht realisiert werden können.

Soweit Systeme, die unter Künstlicher Intelligenz zusammengefasst werden, personenbezogene Daten verarbeiten, betreffen sie auch vielfältige Datenschutzthemen. Dies gilt zum einen für die Erfüllung der allgemeinen Datenschutzgrundsätze wie Fairness, Transparenz, Zweckbindung und Datenminimierung. Sie können auch mit den allgemeinen Verboten der Verarbeitung besonderer Kategorien von personenbezogenen Daten und der automatisierten Entscheidung, die rechtliche oder beeinträchtigende Wirkungen haben können, kollidieren. Zum anderen müssen sie die Datenschutzanforderungen spezifischer Anwendungsbereiche erfüllen, wie etwa des Sozial-, des Polizei-, des Versicherungs-, des Werbe-, des Telekommunikations-, des Internet- oder des Verwaltungsdatenschutzes. Für das Datenschutzrecht stellt sich die Frage, ob Anwendungen der Künstlichen Intelligenz jeweils nur technik- oder bereichsspezifische Problemstellungen verursachen oder ob es übergreifende Fragestellungen gibt, die es rechtfertigen, sie unter dem Begriff der Künstlichen Intelligenz auch aus datenschutzrechtlicher Sicht zusammenzufassen und für unterschiedliche Technikanwendungen allgemeine Anforderungen und Lösungen zu bestimmen.

Zur Regulierung Künstlicher Intelligenz hat die Europäische Kommission am 21. April 2021 den Entwurf einer Verordnung veröffentlicht. In diesem Entwurf hat die Kommission ihre übertriebene Technikneutralität, die sie in der Datenschutz-Grundverordnung verfolgt hat, aufgegeben. Diese hat dort dazu geführt, dass, bezogen auf die Grundsätze der Datenverarbeitung, die Regelung ihrer Zulässigkeit und die Rechte der betroffenen Person etwa die vernachlässigbaren Risiken der Mitgliederliste eines Sportvereins und die exorbitanten Risiken der Profilbildung von Milliarden Menschen durch global agierende Internetkonzerne risikoneutral gleich behandelt werden. Diesen Fehler vermeidet die Kommission in ihrem neuen Entwurf und regelt bereichs- und anwendungsspezifisch, wie unterschiedliche Risiken für Grundrechte durch unterschiedliche Anforderungen an Anwendungen der Künstlichen Intelligenz abgewehrt werden können. Wie dies gelingen kann und wo der Entwurf der Kommission noch verbessert werden muss, wird in der kommenden Zeit intensiv diskutiert werden müssen.

Zu dieser Diskussion wollen die Beiträge im Schwerpunkt dieses Heftes beitragen. Sie sind aus Vorträgen der Veranstaltung „Künstliche Intelligenz und Datenschutz – Wie lassen sich die neuen Herausforderungen bewältigen?" entstanden, die das Competence Center for Applied Security Technology (CAST), das BMBF-Forum „Pri-

vatheit und selbstbestimmtes Leben in einer digitalen Welt" und der Hessische Beauftragte für Datenschutz und Informationsfreiheit gemeinsam am 18. März 2021 virtuell durchgeführt haben. Sie thematisieren wichtige Aspekte jeder Regulierung Künstlicher Intelligenz und greifen den Entwurf der Kommission auch in der vorliegenden schriftlichen Fassung der Vorträge auf.

Der Schwerpunkt informiert über Datenschutzanforderungen und -lösungen für unterschiedliche Anwendungen Künstlicher Intelligenz. Der einleitende Beitrag von *Dieter Kugelmann,* Landesbeauftragter für Datenschutz und Informationsfreiheit Rheinland-Pfalz, erläutert gesellschaftliche und wirtschaftliche Erwartungen an Künstliche Intelligenz und beschreibt sie als Gegenstand politischer Programme und Ziele. Mit Blick auf ihre wichtigsten Einsatzfelder Arbeit, Mobilität, Gesundheit und Sicherheit erörtert er Risiken und offene Fragen ihrer Anwendung. Er zeigt auf, welche Widersprüche zwischen wesentlichen Eigenschaften Künstlicher Intelligenz und den Grundsätzen des Datenschutzes bestehen, die für die Datenschutzaufsicht zu schwierigen Herausforderungen führen.

Die folgenden drei Beiträge befassen sich am Beispiel von Sprachassistenten, Gesichtserkennung und autonomem Fahren mit spezifischen Technikausprägungen. *Christian Geminn,* Universität Kassel, kontrastiert die breite Nutzung von Sprachassistenten mit ihren Auswirkungen auf die Verwirklichungsbedingungen von Grundrechten. Ihr verführerisches Entlastungspotenzial führt zugleich zu einer Machtverschiebung zugunsten ihrer Anbieter. Diese wird dadurch verstärkt, dass Sprachassistenten die datenschutzrechtlich geforderte Transparenz, Datenminimierung und Systemgestaltung unterlaufen. *Gerrit Hornung* und *Sebastian Schindler*, Universität Kassel, erläutern die Chancen und Risiken, die von Methoden der Gesichtserkennung ausgehen. Sie können die Arbeit von Sicherheitsbehörden erleichtern, können aber – insbesondere in Szenarien der Personenfahndung – zu tief in die Grundrechte sehr vieler betroffener Personen eingreifen. Während im Einsatz durch Polizei Szenarien möglich sind, die datenschutzrechtlich zu rechtfertigen sind, erscheint dies bei privaten Geschäftsmodellen schwerer möglich zu sein. Zumindest die Angebote von ClearView AI und Pimeyes, die ein bestimmtes Gesicht mit Millionen oder Milliarden Gesichtsbildern im Internet vergleichen, verstoßen gegen Datenschutzrecht. *Steffen Kroschwald*, Hochschule Pforzheim, untersucht den Einsatz von Künstlicher Intelligenz im autonomen Auto. Dieser verursacht Probleme, die Grundsätze der Datensparsamkeit und der Speicherbegrenzung, der Transparenz und der Nachvollziehbarkeit, der Zweckbindung und der Rechtfertigung der Datenverarbeitung einzuhalten. Der Beitrag zeigt aber auch auf, wie Systemgestaltung, die sich an dem Leitbild einer „human centric AI" orientiert, zu datenschutzgerechten Ergebnissen führen kann. Schließlich plädiert *Christian Djeffal,* Technische Universität München, dafür, für die Gestaltung automatisierter Entscheidungssysteme Art. 22 DSGVO – ähnlich wie Art. 25 DSGVO – als sozio-technische Gestaltungsnorm zu sehen. Nach dieser Neuinterpretation sind die nach Abs. 1 zu schützenden Rechte, Freiheiten und berechtigten Interessen der betroffenen Personen notwendig zu beachtende Kriterien der Systemgestaltung. In einem iterativen Prozess sind automatisierte Entscheidungssysteme auf ihre Folgen für diese Kriterien zu bewerten und durch geeignete Maßnahmen so zu gestalten, bis sie die Rechte, Freiheiten und Interessen ausreichend schützen.

Alle Beiträge kommen – auf unterschiedlichen Wegen und mit unterschiedlicher Gewichtung – zu dem Ergebnis, dass Anwendungen Künstlicher Intelligenz nur dann zu verantworten sind, wenn sie – bei allen Schwierigkeiten – von Anfang an datenschutzgerecht gestaltet sind und insbesondere die Datenschutzgrundsätze erfüllen. Die Erkenntnisse dieser Beiträge sollte der Unionsgesetzgeber bei seiner Verordnung zur Regulierung Künstlicher Intelligenz berücksichtigen.

Alexander Roßnagel