LEGAL REVOLUTIONary
Rechtsmagazin der digitalen Wirtschaft

# KI und Datenschutz – Zwei Seiten einer Medaille

## Eine Bewertung der Chancen und Risiken

Erdem Durmus | Externer Datenschutzbeauftragter | NOTOS Xperts GmbH
Jens Engelhardt | Managing Partner | NOTOS Xperts GmbH

21. Februar 2020

LR 2020, Seiten 9 bis 16 (insgesamt 8 Seiten)

Künstliche Intelligenz ist eine der brisantesten technologischen Entwicklungen unseres Zeitalters. Insbesondere das vielseitig eingesetzte Machine Learning als Teilbereich hiervon wirft bestimmte datenschutzrechtliche Fragen auf. Verarbeitungen von personenbezogenen Daten in Machine Learning Systemen sind möglicherweise intransparent und für die betroffenen Personen mit Risiken verbunden. Auf der anderen Seite sind Wege denkbar, mit denen KI für die Einhaltung datenschutzrechtlicher Vorgaben eingesetzt werden kann. 1

### I. Was ist unter Künstlicher Intelligenz (KI) zu verstehen?

Künstliche Intelligenz (Abkürzung „*KI*"; englisch „*artificial intelligence*" oder „*AI*") ist ein Teilbereich der Informatik und beschäftigt sich mit der Erforschung von Mechanismen des intelligenten menschlichen Verhaltens und der Übertragung dieses Verhaltens auf einen Computer. Es ist schwierig, eine allgemeingültige Definition für den Begriff KI zu finden, weil der Begriff „Intelligenz" unterschiedlichen Definitionsansätzen unterliegt.[1] 2

Eine Hilfestellung kann allerdings die Kategorisierung in starke KI und schwache KI bieten: Die starke KI beschreibt einen Computer bzw. Roboter, der dazu in der Lage ist, jegliche Probleme zu lösen und jegliche Fragen zu beantworten. Zurzeit ist die starke KI noch ein reines Fantasieprodukt und daran wird sich für eine lange Zeit vermutlich auch nichts ändern. 3

Für Theorie und Praxis ist die schwache KI interessant: Dabei handelt es sich um Algorithmen zur Beantwortung einer speziellen Frage unter Anwendung vorher selbst erlernter Lösungswege. Die schwache KI unterscheidet sich von einem regelbasierten Programm („Wenn dies → dann jenes") dadurch, dass sie selbst lernt, also mit bisher unbekannten Daten und Informationen arbeitet und eigenständig Muster findet. Somit 4

[1] https://www.spektrum.de/lexikon/neurowissenschaft/kuenstliche-intelligenz/6810

kann KI auf unbekannte Situationen reagieren und auf Basis von Erfahrungswerten arbeiten. [2]

KI hat verschiedene Erscheinungsformen und wird sehr vielseitig eingesetzt. Das Machine Learning ist beispielsweise eine Automatisierung für die Erstellung analytischer Modelle. Mit verschiedenen Praktiken aus neuronalen Netzen, Operations-Research, Statistik und Physik werden in Daten versteckte Erkenntnisse gesucht. Dabei wird in den Systemen nicht programmiert, an welchen Stellen gesucht werden soll oder welche Schlussfolgerungen gezogen werden sollen. Das neuronale Netz ist eine Ausprägung des maschinellen Lernens. Es besteht aus miteinander verbundenen Knoten bzw. Neuronen, die zur Informationsverarbeitung auf externe Dateneingänge reagieren und Informationen zwischen den einzelnen Knoten weiterleiten. Dabei sind mehrere Durchläufe notwendig, um Verbindungen zu finden und undefinierte Daten zu gewichten. [3] 5

Die Vorstellung ist, dass das IT-System in der Lage ist, auf Basis vorhandener Datenbestände und vorgegebener Algorithmen selbstständig Muster und Gesetzmäßigkeiten zu erkennen und Lösungen zu entwickeln. Grundsätzlich wird zwischen fünf Arten des Machine Learnings unterschieden: 6

- **Überwachtes Lernen:** Definition und Spezifizierung von Beispielmodellen zur Zuordnung der Informationen entsprechend den Modellgruppen der Algorithmen.
- **Unüberwachtes Lernen:** Automatisierte Bildung von Modellgruppen auf Basis eigenständig erkannter Muster.
- **Teilüberwachtes Lernen:** Mischung aus überwachtem und unüberwachtem Lernen.
- **Bestärkendes Lernen:** Feedback durch Belohnungen und Bestrafungen (Interaktion).
- **Aktives Lernen:** Algorithmus hat die Möglichkeit, für bestimmte Eingangsdaten die gewünschten Ergebnisse zu erfragen. Dabei begrenzt der Algorithmus die Fragen auf solche, die eine Ergebnisrelevanz haben.

Neben dem Machine Learning gibt es weitere KI-basierte Technologien, etwa die Automatisierung, Robotik, Machine Vision, Natural Language Processing (NLP) oder die Mustererkennung. Für datenschutzrechtliche Fragestellungen ist das Machine Learning allerdings am interessantesten, weshalb sich dieser Beitrag auf diesen Teilbereich konzentriert. 7

[2] https://www.wfb-bremen.de/de/page/stories/digitalisierung-industrie40/was-ist-kuenstliche-intelligenz-definition-ki
[3] https://www.sas.com/de_de/insights/analytics/what-is-artificial-intelligence.html#used

## II. Datenschutzrechtliche Fragen von Machine Learning

Machine Learning wird auf Basis von großen Datenmengen trainiert, wodurch es in die Lage versetzt werden soll, eigenständig Muster und Gesetzmäßigkeiten zu erkennen.[4] Durch Beispiele lernt der Computer, eigenständig Lösungen für unbekannte Probleme zu finden, ohne vorher dafür programmiert worden zu sein.[5] 8

### 1. Machine Learning und Betroffenenrechte

Für den Betrieb von Machine Learning wird KI nicht nur mit Sachdaten gespeist, sondern auch mit personenbezogenen Daten. Zur Veranschaulichung genügt ein einfaches Beispiel: Eine KI-gestützte Software soll Kundenanfragen technischer Art an den richtigen Support-Mitarbeiter weiterleiten. Für diesen Zweck nutzt das System Informationen aus der Anfrage und generiert daraus Tickets. Um die Richtigkeit der Weiterleitung zu gewährleisten, trainiert sich das System selbst auf Basis der eingespeisten Daten. 9

Art. 15 ff. DSGVO normieren die datenschutzrechtlichen Betroffenenrechte. Die Bearbeitung von Betroffenenrechten ist grundsätzlich kein besonderer Vorgang, sondern folgt einer vordefinierten Struktur: 10

1. Anfrage der betroffenen Person geht ein
2. Weiterleitung der Anfrage an den zuständigen Mitarbeiter
3. Überprüfung der Identität der betroffenen Person
4. Mitteilung über das Ergebnis der Identitätsfeststellung
5. Heraussuchen der erforderlichen Datensätze
6. Umsetzung der Anfrage
7. Mitteilung an die betroffene Person (positiv oder negativ)

Diese chronologische Abfolge der o.g. Schritte bietet grundsätzlich erst dann einen Mehrwert, wenn der Verantwortliche sicher sein kann, dass alle fraglichen Datenspeicherorte erfasst sind und durchsucht werden können. Entsprechend müsste die Datenhaltung beim Verantwortlichen strukturiert und zugänglich sein. 11

Wenn die Daten allerdings nicht mehr zu finden sind oder erst gar nicht erreichbar sind, dann stellt dies den Verantwortlichen vor neue Herausforderungen. In der logischen Konsequenz können die Betroffenenrechte nicht sachgemäß bearbeitet werden. Zur Veranschaulichung dieses Problems kann das o.g. Beispiel wieder aufgegriffen werden: Das KI-System zur Weiterleitung der Kundenanfragen extrahiert Inhalte aus dem Nachrichtentext der Anfrage und der Betreffzeile und versucht, anhand dieser 12

[4] Gausling, DSRITB 2018, 522.
[5] Gausling, ZD 2019, 335.

Informationen den Sachverhalt der Anfrage zu erfassen. Zudem werden die Kontaktdaten sowie der Vor- und Nachname des Kunden erfasst und mit vorhandenen Datensätzen abgeglichen. All diese Informationen werden innerhalb eines neuronalen Netzes an einzelne Knoten weitergegeben.

Im KI-basierten Ticketsystem befinden sich personenbezogene Daten von einer Vielzahl von Personen, die für den Verantwortlichen möglicherweise nicht mehr identifizierbar sind. Wenn ein Kunde beispielsweise ein Auskunftsrecht nach Art. 15 DSGVO geltend macht, kann der Verantwortliche Daten aus diesem KI-System nicht mehr berücksichtigen. 13

An dieser Stelle findet Art. 11 Abs. 2 DSGVO Anwendung. Nach dieser Vorschrift muss der Verantwortliche die betroffene Person unterrichten, wenn er nachweisen kann, dass er nicht in der Lage ist, sie zu identifizieren. Dies betrifft zum einen den Fall, dass der Verantwortliche nicht weiß, ob überhaupt personenbezogene Daten vom Antragsteller verarbeitet werden. Zum anderen betrifft dies den Fall, dass der Verantwortliche zwar weiß, von welchen betroffenen Personen Daten verarbeitet werden, diese aber nicht individuell zuordnen kann.[6] 14

Der Verantwortliche muss der betroffenen Person gegenüber darlegen können, dass er nicht in der Lage ist, diese zu identifizieren bzw. ihr entsprechende Datensätze eindeutig zuzuordnen. Dabei muss er ihr genau mitteilen, welche Vorschriften er nicht einhalten kann und aufgrund welcher fehlenden Daten dies nicht möglich ist. Denn erst nach diesen Informationen ist die betroffene Person in der Lage, einzuschätzen, welche Daten dem Verantwortlichen zur Bearbeitung der Anfrage noch fehlen. Verfügt der Verantwortliche über keinerlei Kontaktdaten der betroffenen Person, so fällt seine Informationspflicht weg. [7] 15

## 2. Machine Learning zur Umsetzung der Löschvorgaben

Die regelkonforme, turnusgemäße Löschung von personenbezogenen Daten, deren Zweck erfüllt ist (End of Purpose) und deren etwaige gesetzliche Aufbewahrungspflicht abgelaufen ist, stellt Unternehmen vor große Herausforderungen: Zum einen ist es je nach Applikation durchaus komplex, Stammdaten und Bewegungsdaten einer Person oder eines Geschäftsvorfalls zu löschen. Zum anderen unterliegen personenbezogene Daten unterschiedlichen Aufbewahrungsfristen, wie z.B.: 16

- 72 Stunden (Videoüberwachung)
- 6 Monate (nicht erfolgreiche Bewerbungen)
- 1 Jahr (Ausdruck einer Fahrerkarte von Kraftfahrern)
- 2 Jahre (Prüfergebnisse von Feuerlöschern durch Sachkundigen)

[6] Wolff, in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 11 DSGVO, Rn. 22.
[7] Kampert, in: Sydow, DSGVO Kommentar, Art. 11 DSGVO, Rn. 11.

- 3 Jahre (Daten aus Abfallverfahren)
- 5 Jahre (Dokumentation von Erste-Hilfe-Leistungen, Baudokumentationen)
- 6 Jahre (Handelsbriefe)
- 10 Jahre (Handelsbücher, Rechnungen und Buchungsbelege)
- 15 Jahre (Proben und Abschlussbericht jeder Prüfung nach ChemG)
- 30 Jahre (Personaldaten zu Ansprüchen auf Versorgungszusage, Stammrecht, Anspruch auf vertragliche oder gesetzliche Erhöhung der Rente; Titel; Ansprüche aus dinglichen Rechten)
- 40 Jahre (Verzeichnis über Arbeitnehmer, die Tätigkeiten ausführen, bei denen sie Asbeststaub oder Staub von asbesthaltigen Materialien ausgesetzt sind oder sein können; Ärztliche Unterlagen zur arbeitsmedizinischen Vorsorge nach ArbMedVV)
- Unbegrenzt (Prüfaufzeichnungen und Prüfbescheinigungen nach BetrSichV)

Die Folge dieser Komplexität ist, dass entweder gar nicht oder pauschaliert nach beispielsweise 15 Jahren in Unternehmen gelöscht wird, wenn nicht umfangreiche Löschprojekte, meist verbunden mit dem Erwerb von Zusatzmodulen, aufgesetzt werden.

An dieser Stelle können mit künstlicher Intelligenz ausgestattete Systeme für Unternehmen hilfreich sein, wenn sie in der Lage sind, personenbezogene Daten automatisch zu kategorisieren und mit Löschattributen zu versehen. Ob das System – quasi paternalistisch – die Löschung dann auch selbstständig vornehmen oder Daten nur zur Löschung vorschlagen soll, muss freilich der Einschätzungsprärogative des Unternehmens (Datenvolumen, Personalaufwand, Risiko falscher Löschungen) vorbehalten bleiben. 17

Der nächste konsequente, wenn auch exponentielle Schritt, dürfte dann sein, dass KI personenbezogene Daten aus sich selbst heraus löscht und durch jüngere, aktuellere Daten ersetzt, sobald eine Löschpflicht besteht. 18

### 3. Datenschutz-Folgenabschätzungen für Machine Learning

Die Datenschutz-Folgenabschätzung (nachfolgend DSFA) ist in Art. 35 DSGVO geregelt und verpflichtet den Verantwortlichen dazu, eine Abschätzung der Folgen von Verarbeitungsvorgängen durchzuführen, sofern sie aufgrund der Art, des Umfangs der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben. 19

Art. 35 Abs. 3 DSGVO zählt beispielhaft Fälle auf, bei deren Vorliegen in jedem Fall eine DSFA durchzuführen ist. 20

Diese sind:

- Die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen (lit. a)
- Die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (lit. b)
- Die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (lit. c)

Des Weiteren regelt Art. 35 Abs. 4 DSGVO die Pflicht von Aufsichtsbehörden, eine Liste von Verarbeitungstätigkeiten zu erstellen und zu veröffentlichen, für die auf jeden Fall eine DSFA durchzuführen ist (sog. Positivliste). Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz; DSK) hat eine solche Liste veröffentlicht, welche auch auf den Webseiten von einzelnen Datenschutzbehörden verfügbar ist.[8]

Die Positivliste umfasst derzeit 17 Einträge und ist angelehnt an das WP 248 der Art. 29-Datenschutzgruppe.[9] Doch das Fehlen eines Verarbeitungsvorganges heißt nicht automatisch, dass für diese Verarbeitung keine DSFA durchzuführen wäre. Vielmehr müssten die neun Kriterien der Art. 29-Datenschutzgruppe berücksichtigt und auf die fragliche Verarbeitung angewendet werden. Diese neun Kriterien sind: 21

1. Bewerten oder Einstufen
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. Systematische Überwachung
4. Vertrauliche Daten oder höchstpersönliche Daten
5. Datenverarbeitung in großem Umfang
6. Abgleichen oder Zusammenführen von Datensätzen
7. Daten zu schutzbedürftigen Betroffenen
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Fälle, in denen die Verarbeitung an sich die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert

[8] DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist. https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/DSK_DSFA_Muss-Liste_Version_1_1_Deutsch.pdf

[9] Art. 29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, https://www.datenschutz-bayern.de/technik/orient/wp248.pdf

Eine DSFA wird dann obligatorisch, wenn mindestens zwei dieser Punkte zutreffen. Bezogen auf das Beispiel mit dem KI-basierten Ticketsystem wären das zumindest die Punkte 5, 6, 8 und wahrscheinlich auch 9.

Dass beim Machine Learning eine „Datenverarbeitung in großem Umfang" stattfindet, liegt in der Natur der Sache. Um verlässliche Ergebnisse zu liefern, benötigt Machine Learning einen großen Pool an Erfahrungswerten. Diese Erfahrungswerte können eben nur mit reichen Datenbeständen genährt werden. Das Machine Learning steht bereits vom Konzept her den Grundsätzen der Datenminimierung und Speicherbegrenzung entgegen. 22

Ein weiterer und wichtiger Punkt, den es hervorzuheben gilt, ist die „innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen". Als Beispiele führt die Art. 29-Datenschutzgruppe die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zwecke der verbesserten Zugangskontrolle sowie ganz allgemein Anwendungen aus dem Bereich „Internet der Dinge" an. 23

Risiken für die Rechte und Freiheiten der betroffenen Personen können sich bereits dadurch ergeben, dass „neuartige Formen der Datenerfassung und -nutzung" mit ihnen einhergehen. Dies trifft auf das Machine Learning zu. Es handelt sich um eine neue Methode, die jedem Datensatz eine eigene Bedeutung zumisst und auf nie dagewesene Weise aus dem Zusammenspiel von Datensätzen Schlussfolgerungen zieht. 24

Beispiel: Aufgrund einer hohen Nachfrage an Mietwohnungen beschließt ein Maklerunternehmen, eine KI-gestützte Software einzusetzen, die potenzielle Neumieter auf Basis ihres Namens und ihres aktuellen Wohnortes selektieren soll. Damit soll gewährleistet werden, dass nur zahlungsfähige Mieter in die Wohnungen einziehen. Das Machine Learning wird vorab mit Daten eingespeist und nach dem Prinzip des bestärkenden Lernens trainiert; es wird also rückgemeldet, ob eine Entscheidung gut war oder nicht. 25

Durch den Einsatz dieser Software werden bestimmte Personengruppen von vornherein von der Auswahl ausgeschlossen. Persönliche Aspekte, insbesondere ihr Aufenthaltsort werden bewertet und ihnen entsteht zumindest ein gesellschaftlicher Nachteil, so wie EG 75 DSGVO es beschreibt. Auch in dem „Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen" wird auf dieses Risiko hingewiesen. Es heißt, dass insbesondere bei neuronalen Netzen nicht ausgeschlossen werden kann, dass Menschen mit bestimmten Eigenschaften benachteiligt oder ungerecht bevorteilt werden. Das Problem hierbei ist, dass diese „unerwünschte Diskriminierungseigenschaft" von außen nicht ersichtlich ist.[10] 26

[10] DSK, Positionspapier der DSK: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2019/2019-DSK-Positionspapier_Kuenstliche_Intelligenz.pdf

### III. Fazit

Wie in vielen Bereichen ist Künstliche Intelligenz oder Machine Learning für den Datenschutz Bedrohung und Chance zugleich. Einerseits läuft die Notwendigkeit KI-Systeme mit einer möglichst großen Menge von relevanten Daten zu füttern, naturgemäß Grundprinzipien aus der DSGVO der Datensparsamkeit und Datenminimierung zuwider. 27

Andererseits kann KI sehr wohl dazu beitragen, dass Unternehmen die Erfüllung von Datenschutzgrundpflichten und Betroffenenrechten effizienter gelingt als ohne KI.