

01.19

PinG

Privacy in Germany

Datenschutz und Compliance

7. Jahrgang
Januar 2019
Seiten 1–48

www.PinGdigital.de

Herausgeber:

Prof. Niko Härting

Redaktion:

*Dr. Sebastian J. Golla
Dr. Niclas Krohm
Dr. Carlo Piltz
Sebastian Schulz*

Ständige Mitarbeiter:

*Dr. Simon Assion
Dr. Jana Moser
Philipp Müller-Peltzer
Frederick A. Richter, LL. M.
Prof. Dr. Jan Dirk Roggenkamp
Daniel Schätzle
Dr. Rainer Stentzel
Jan-Christoph Thode*

**PRIVACY
TOPICS**

H.-C. Gräfe

Webtracking und Microtargeting als Gefahr für
Demokratie und Medien

P. Krause

Datenportabilität – Pflichten für Verantwortliche im
Rahmen des Rechts auf Datenübertragbarkeit (Teil 2)

I. L. Selz

Zuordnung und Transaktion von Geschäfts-
geheimnissen im Informationszeitalter

G. Dimitrov/D. Ilieva/R. Makshutova

What data protection rights do employees have in
2018 – The right to personal life, the GDPR and the
balance of interests

I. Alexe/D.-M. Şandru

National Regulations Aimed at Applying the GDPR
in Romania

**PRIVACY
COMPLIANCE**

T. Britz/M. Indenhuck

The Usual Others – Third-Party Data in Contracts

**PRIVACY
NEWS**

J. Caspar

Herrschaft der Maschinen oder Herrschaft des Rechts?
– Grenzen und Leitlinien für algorithmische und
selbstlernende Verfahren in der Verwaltung – Thesen

PRIVACY NEWS

Herrschaft der Maschinen oder Herrschaft des Rechts?

Grenzen und Leitlinien für algorithmische und selbstlernende Verfahren in der Verwaltung – Thesen

Prof. Dr. Johannes Caspar

I. Einleitung

Die Digitalisierung der Verwaltung und der städtischen Infrastrukturen nimmt langsam aber sicher Fahrt auf. Projekte der Online-Antragstellungen von Kindergeld über Wohngeld bis hin zum Bewohnerparken ermöglichen es, Verwaltungsverfahren von zuhause anzustoßen und sind damit vorbildlich in Bezug auf die Bürgerfreundlichkeit. Auch die Digitalisierung städtischer Infrastrukturen, etwa durch intelligente Verkehrsleit- und Parkraumsysteme, kann zu erheblichen Effizienzsteigerungen und energetischen Einsparungen führen und damit einen zentralen Schlüssel für eine nachhaltige Stadtentwicklung darstellen.

Den Chancen, die sich an die Digitalisierung knüpfen, stehen aber auch immense Risiken gegenüber, die sich daraus ergeben, dass die Steuerung der modernen Verwaltung und städtischer Infrastrukturen über die massenhafte Verarbeitung von ganz unterschiedlichen Daten von Bürgerinnen und Bürgern erfolgt.

Darüber hinaus kommt ein weiterer Aspekt in Betracht, der bislang kaum beleuchtet wird: In der Diskussion über die moderne Verwaltung und städtische Infrastrukturen steht immer stärker die Einbeziehung von Algorithmen und Künstlicher Intelligenz im Vordergrund. Die Einsatzfelder reichen hier vom vollautonomen

Fahren über die Gesichtserkennung in Echtzeit bis hin zum Einsatz von selbstlernender Software, die Prognosen über das individuelle Verhalten von Personen in unterschiedlichen Zusammenhängen, von der öffentlichen Sicherheit bis hin zum Kindeswohl in Familien, ermöglichen oder sie betreffen lediglich den Einsatz von Spam-Filtern in der Verwaltung.

Dieser Diskussion vorgelagert ist in jedem Fall das Erfordernis einer terminologischen Klärung der zugrundeliegenden Begriffe. Hier geht es gerade darum, ein terminologisches Verständnis für Künstliche Intelligenz zu finden, ohne das eine rechtliche Einordnung nicht möglich ist.

1. Das Begriffspaar Algorithmische Entscheidung/Künstliche Intelligenz

Algorithmische Entscheidungen laufen grundsätzlich deterministisch ab und sind dadurch gekennzeichnet, dass bei Bestehen derselben Voraussetzungen stets das gleiche Ergebnis erzielt wird.

Im Gegensatz zu derartigen Konditionalprogrammen handelt es sich bei Verfahren, die auf dem Einsatz Künstlicher Intelligenz beruhen, grundsätzlich um entwicklungs-offene Prozesse, bei denen ein unterschiedliches Maß an Autonomie innerhalb des Systems ein Fortschreiben des Algorithmus selbsttätig generiert. Im Wesentlichen geht



Prof. Dr. Johannes Caspar,
Hamburgischer Beauftragter für Datenschutz
und Informationsfreiheit

es dabei um verschiedene Formen des maschinellen Lernens, das jeweils Muster und Gesetzmäßigkeiten erkennt. Das selbstlernende System optimiert sich durch die Erfahrung und ist auch in der Lage, für unbekanntere Szenarien Lösungen zu finden.

Dabei sind zwei Stufen selbstlernender Systeme zu unterscheiden: solche, bei denen das maschinelle Lernen grundsätzlich vor dem Praxiseinsatz abgeschlossen ist und solche, bei denen eine Anpassung der Algorithmen fortdauernd während des Echtbetriebs erfolgt. Dabei sind die letzteren Systeme mit Blick auf Vorhersehbarkeit der Entscheidungen besonders kritisch zu sehen, da die opaken Strukturen weder eine vorgängige noch eine nachträgliche Kontrolle des sich selbst überlassenen Systems mit transparenten Vorgaben ermöglichen.

Gerade im Bereich der öffentlichen Verwaltung werfen selbstlernende Verfahren nicht nur unter dem Aspekt demokratischer Legitimation und rechtsstaatlicher Kontrolle Fragen auf, sondern erweisen sich in hohem Maße für die Verwirklichung der Grundrechte, insbesondere des Grundrechts auf informationelle Selbstbestimmung nach Art. 1 GG i.V.m. Art. 2 Abs. 1 GG bzw. den Grundrechten auf Datenschutz sowie der Achtung der Familie und Privatsphäre (Art. 7 und Art. 8 GrCh) als problematisch.

Anders als bei rein algorithmischen Entscheidungen ist bei selbstlernenden Systemen ein Zurechnungszusammenhang nicht oder nur sehr schwer herstellbar. Automatisierte Einzelentscheidungen sind in diesem Bereich nicht zwingend an eine vorgegebene Struktur von Tatbestand und Rechtsfolge geknüpft, da sich regelmäßig die maschinellen Lernprozesse zwischen Normbefehl und Entscheidung legen. Ein bruchloses Abbilden von normlogischen Strukturen im Rahmen von informationstechnischen Konditionalprogrammen ist hier nicht möglich. Autonome Systeme sind daher von außen betrachtet indifferent zu den von ihnen bewirkten Folgen. Eine Ableitbarkeit des Eingriffsakts aus gesetzlichen Vorgaben – Wesensmerkmal demokratischer Rechtsstaatlichkeit für den Eingriff in die Grundrechte – steht daher grundsätzlich in Frage. Wo eine von einer rationalen Begründung getragene Nachvollziehbarkeit nicht besteht, lässt sich eine Entscheidung nicht mehr einer rechtsstaatlichen Kontrolle unterziehen. Ohne die Nachprüfbarkeit von staatlichem Handeln anhand einer gesetzlichen Eingriffsnorm bleibt das Recht auf der Strecke und weicht einer intransparenten Maschinenentscheidung.

Maschinelles Lernen beruht zudem auf einem permanenten Training anhand von Echtdateien. Derartige Verfahren gelten als voreingenommen (biased), weil sie auf einer empirischen Datenbasis beruhen, die nicht neutral ist, sondern bereits auf einer in bestimmter Weise vorgeformten Realität basiert. Der Einsatz von Künstlicher Intelligenz kann daher im Kern zu falschen Annahmen führen, aus denen sich massive diskriminierende Folgen für die davon Betroffenen ergeben, ohne dass dies überhaut erkennbar wird.

2. Selbstexekutive und unterstützende Systeme des maschinellen Lernens

Innerhalb des weiten Bereichs automatisierter Entscheidungen, die auf Basis von Algorithmen oder selbstlernenden Systemen erfolgen, ist wiederum zu differenzie-

ren zwischen Entscheidungen, die sich direkt aus maschinellen Prozessen ergeben und solchen, die durch den menschlichen Entscheider getroffen werden. Während sich die selbst vollziehende maschinelle Entscheidung nicht mehr über eine ununterbrochene demokratische Legitimationskette von einer durch den Gesetzgeber erlassenen Norm auf einen menschlichen Entscheider zurückführen lässt, bleibt die maschinelle Verarbeitung, die lediglich individuelle Entscheidungen vorbereiten hilft, lediglich eine Entscheidungsgrundlage für menschliche Subjekte. Die rechtsstaatlichen Vorgaben einer demokratisch legitimierten Entscheidung auf gesetzlicher Grundlage sind hier durchaus erkennbar.

3. Zwischenfazit

Eine Überwachung selbstlernender Systeme durch inneradministrative Prozesse oder durch unabhängige Stellen von außen wird insoweit wesentlich erschwert, als diese sich autonom fortentwickeln. Das geht einher mit einer mangelnden Transparenz der Datenverarbeitung. Deren Ergebnisse werden zwar bekannt, soweit die Verarbeitung zu Entscheidungen über Einzelfälle führt. Die innere Struktur und Logik, mit der dies geschieht, bleiben jedoch regelmäßig im Dunkeln. Insoweit stellt die Künstliche Intelligenz, die über Rechtsgüter von Menschen und über die Verwirklichung von Grundrechten entscheidet, eine regelungsbedürftige Risikotechnologie dar.

Die folgenden Ausführungen sind vor allem auf den Einsatz von autonom lernenden Systemen bezogen. Dabei wird nicht verkannt, dass auch „einfachen“ algorithmenbasierten Entscheidungen immer ein hohes Diskriminierungspotential innewohnt, dem die Rechtsordnung Grenzen setzt. So z.B., wenn ein Algorithmus stochastische Zusammenhänge zur Herkunft einer Person oder ihrer Glaubenszugehörigkeit heranzieht und seine Entscheidung hieran ausrichtet. Dass Entscheidungen auf Grundlage derartiger Merkmale nicht zu einer Ungleichbehandlung führen dürfen, ergibt sich nicht zuletzt bereits aus dem Grundsatz der Nichtdiskriminierung Art. 21 Abs. 1 GrCh und Art. 3 Abs. 3 GG. Aber auch die DSGVO zieht der Verarbeitung derartiger besonderer Kategorien personenbezogener Daten enge Grenzen: Sie sind nur auf Grundlage einer Einwilligung oder besonderer öffentlicher Interessen zulässig (Art. 9 Abs. 2 DSGVO).

Für algorithmenbasierte Entscheidungen der Verwaltung, die durch automatisierte Systeme getroffen werden dürfen, hat der Gesetzgeber in § 155 IV AO, § 31a SGB X

und § 35a VwVfG bereits Regelungen geschaffen. Diese Regelungen beziehen sich lediglich auf gebundene Entscheidungen der Verwaltung, sodass regelmäßig der Einsatz von selbstlernenden Systemen nicht in Betracht kommt. Vorhersehbarkeit und Ableitbarkeit von deterministischen Entscheidungen, etwa im Bereich des Steuerbescheids, eröffnen lediglich die Abbildung des gesetzlichen Normenprogramms. Derartige von der Verwaltung eingesetzte Automationsprozesse lassen sich daher relativ unproblematisch auf die Bindung der Exekutive an Recht und Gesetz wie auch auf eine demokratische Legitimationskette von Organen der Gesetzgebung bis hinab zu automatisierten Entscheidungen zurückführen. Die Steuerbarkeit derartiger Entscheidungen durch deterministische Verfahren ist daher weit weniger problematisch als im Bereich von selbstlernenden Systemen.

II. Entscheidungen selbstlernender Systeme, die unmittelbar automatisiert erfolgen

Für die Kategorien der selbstvollziehenden automatisierten Entscheidungen erfüllt das sekundäre Gemeinschaftsrecht in Art. 22 DSGVO die Funktion des Gesetzesvorbehalts (vgl. Art. 20 Abs. 1 GG; Art. 52 Abs. 1 GrCh). Danach ergibt sich für automatisierte Einzelfallentscheidungen – unabhängig davon, ob diese aufgrund von selbstlernenden Systemen erfolgen oder algorithmenbasiert sind – sowohl im EU- als auch für das nationale Recht das Erfordernis einer gesetzlichen Eingriffsnorm.

Danach besteht ein grundsätzliches Verbot für Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen und den Betroffenen gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (Art. 22 Abs. 1 DSGVO). Ausnahmen hiervon ergeben sich jedoch zur Erfüllung eines Vertrages oder nach ausdrücklicher Einwilligung der Betroffenen. Der Einsatz von Künstlicher Intelligenz und Algorithmen kommt ferner in Betracht, wenn die Entscheidung aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten ergeht und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Pflichten sowie der berechtigten Interessen der betroffenen Personen enthalten (Art. 22 Abs. 2 lit. b) DSGVO). Erfasst hiervon sind allerdings nur solche automatisierten Entscheidungen, die gegenüber Betroffenen rechtliche Wirkung entfalten oder deren Rechte erheblich beeinträchtigen.

Bei automatisierten Entscheidungen zur Erfüllung eines Vertrags oder auf Grundlage einer Einwilligung ist zudem zu berücksichtigen, dass dem Betroffenen immer das Recht zustehen muss, dass der Verantwortliche in die Entscheidung eingreift (Art. 22 Abs. 3 DSGVO). Dabei muss der Betroffene seinen eigenen Standpunkt darlegen können (Art. 22 Abs. 3 DSGVO).

Prominentestes Beispiel für ein selbst-exekutives selbstlernendes System ist das vollautonome Fahren, das in Echtbetrieb im Rahmen der städtischen Infrastruktur zunächst in Pilotverfahren erprobt werden soll. Während die umfassende Vernetzung von Verkehrsteilnehmern (Car to X-/Car to Car-Kommunikation) ohnehin einer datenschutzrechtlichen Rechtsgrundlage als Legitimation zur umfassenden Verarbeitung, insbesondere der Erhebung, Speicherung und Übermittlung, von personenbezogenen Daten aus dem Verkehrsgeschehen heraus bedarf, bringt der Einsatz von voll-autonomen Kfz weitergehende Anforderungen für den Einsatz autonom lernender Systeme mit sich.

Die Debatte um das autonome Fahren wird bestimmt durch das utilitaristische Argument, wonach das autonome Fahren zu einer deutlich steigenden Verkehrssicherheit und sinkenden Unfallzahlen führen wird. Doch selbst bei Entscheidungen, die über alle Daten von Verkehrsteilnehmern verfügen, wird es nicht zu vermeiden sein, dass im Einzelfall auch in Rechte Betroffener eingegriffen wird. Das folgt letztlich aus der Tatsache, dass mit der Existenz von Menschen, die als Fußgänger oder Fahrradfahrer ohne digitale Fahrsysteme am Straßenverkehr beteiligt sind, individuelle Fehler nicht zu vermeiden sind.

Daher besteht das Risiko für jeden Verkehrsteilnehmer, dass aus der automatisierten Verarbeitung auch der eigenen Daten unmittelbar maschinelle Entscheidungen resultieren, die zu körperlicher Verletzung oder sogar dem Tod im Straßenverkehr führen können.

Hier gibt es daher einen rechtlichen Handlungsbedarf, angemessene Maßnahmen zur Wahrung von Rechten und Freiheiten betroffener Personen zu treffen, und zwar bevor die Systeme eingesetzt werden. Das folgt aus der gesetzlichen Umsetzungsverpflichtung in Art. 22 Abs. 2 lit. b) DSGVO und legt gerade für autonom lernende Systeme, deren Entscheidungen in Rechte betroffener Personen eingreifen, rechtlich verbindliche Vorgaben fest.

Um diese Vorgaben umzusetzen, ergeben sich verschiedene flankierende Maßnahmen sowohl aus bereits bestehenden Nor-

men als auch nach Maßgabe von neu zu schaffenden Rechtsnormen:

- Zulassungs- und begleitende Kontrollverfahren: Offenlegungspflichten und Kontrollmöglichkeiten sichern den Grundsatz der Letztverantwortlichkeit menschlichen Verhaltens, alle automatisierten Entscheidungen müssen daher durch natürliche oder juristische Personen verantwortet werden. Die Einführung autonomer Systeme wirft insoweit nicht ausschließlich ethische Fragen auf, sondern setzt auch rechtliche Bewertungen im Rahmen eines bestimmten Zulassungsverfahrens und eine begleitende Kontrollverantwortlichkeit öffentlicher Stellen voraus. Diese sind verbindlich zu schaffen und ergeben sich aus einer grundrechtlichen Schutzpflicht gegenüber den vom Einsatz selbstlernender Systeme potentiell betroffenen Rechtssubjekten.

Es bedarf ferner:

- Transparenter Information und Auskunftsrechte über das Verfahren der automatisierten Entscheidungsfindung (Art. 12, Art. 13, Art. 14, Art. 15 DSGVO). Jede automatisierte Verarbeitung löst nach Art. 14 Abs. 3 lit. g) DSGVO die Pflicht aus, über die involvierte Logik sowie Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person aussagekräftig zu informieren.
- Der Einhaltung der Grundsätze von Privacy by Default und Privacy by Design nach Art. 25 Abs. 1 und Abs. 2 DSGVO sowie der Berücksichtigung der technisch-organisatorischen Maßnahmen zur Datensicherheit nach Art. 32 DSGVO.
- Der Beachtung des Grundsatzes der Zweckbindung dahingehend, dass Daten, die bei der Verarbeitung anfallen, nicht in einer mit dem Erhebungszweck nicht zu vereinbarenden Weise weiterverarbeitet werden (vgl. Art. 5 Abs. 1b, Art. 6 Abs. 3 lit. b) DSGVO).
- Der Vornahme von Datenschutzfolgenabschätzungen, ggfs. mit vorheriger Konsultation der Aufsichtsbehörde (Art. 35, Art. 36 DSGVO) mit einer bislang noch nicht geregelten Veröffentlichungspflicht.

III. Entscheidungen vorbereitende automatisierte Datenverarbeitungen

Eine weniger eindeutige rechtliche Zuordnung im geltenden Recht als bei voll-

automatisierten selbstexekutiven Entscheidungen ergibt sich für automatisierte Verarbeitungsprozesse, die Entscheidungen für öffentliche Stellen lediglich vorbereiten. Hier fehlt es regelmäßig an einer maschinell erzeugten Einzelfallentscheidung, sodass die qualifizierten Vorgaben über Art. 22 Abs. 1 DSGVO jedenfalls nicht direkt anwendbar sind.

Die auf der Basis von selbstlernenden Systemen künftig berechneten Wahrscheinlichkeiten etwa von sicherheitsrelevanten Vorfällen bzw. der Profilbildung von Menschen (Predictive Policing/automatisierte Gesichtserkennung in Echtzeit zu Fahndungszwecken) oder z.B. von Bewährungsprognosen, die über vorläufige Haftentlassungen bzw. die Verhängung von Bewährungsaufgaben von Personen entscheiden, sind zunächst lediglich maschinell erstellte Prognosen ohne direkte Rechtsfolgen. Sie stellen für die rechtliche Beurteilung weniger voraussetzungsvolle Szenarien dar.

Obwohl Entscheidungen durch den zuständigen Funktionsträger in dieser Fallgruppe nicht unmittelbar durch maschinelle Vorgaben determiniert werden, entsteht durch die immanente Maschinenlogik der Datenverarbeitung eine Prima-Facie-Evidenz, die es den Entscheidern regelmäßig erschwert, ohne die Übernahme eigener Argumentations- und Beweislasten von den maschinell berechneten Prognosen abzuweichen. In einer von selbstlernender Software geprägten Verwaltungspraxis ist daher zu erwarten, dass sich der Grundsatz in dubio pro machina etablieren und zu einer weitreichenden faktischen Geltung maschineninduzierter Entscheidungen führen wird.

Der konsultative Einsatz von Künstlicher Intelligenz beruht in hohem Maße auf der Verarbeitung von personenbezogenen Daten. Hierfür bedarf es regelmäßig einer rechtlichen Grundlage. Dies betrifft Erhebung und Speicherung von Daten, aber auch die daran anschließende Verarbeitung der Daten durch selbstlernende Systeme. Bereits das Sammeln und Matchen von Daten zu dem jeweils verfolgten Zweck kann, wie im Bereich des Predictive Policing, wo die verfassungsrechtliche Unschuldsvermutung und letztlich auch die Menschenwürde einen personenbasierten Einsatz der Auswertung von Big Data ohnehin limitieren, unzulässig sein.

Für die auf dieser ersten Ebene zulässigen Datenverarbeitungen für bestimmte Eingriffszwecke sind beim Einsatz von selbstlernenden Systemen grundsätzlich weitergehende Maßnahmen für eine transparente Information und Auskunft der von

der Datenverarbeitung betroffenen Personen nach Maßgabe der Art. 12 ff. der DSGVO bzw. nach Maßgabe von bereichsspezifischen Regelungen, etwa der JI-Richtlinie (Richtlinie EU 2016/680) für die Verarbeitung von Daten zum Zweck der Strafverfolgung oder der Gefahrenabwehr, erforderlich.

Da mangels einer maschinellen Entscheidung nicht direkt die Anforderungen des Art. 22 DSGVO gelten, kommt in dieser Fallgruppe nur eine entsprechende Anwendung der Regelungen zur Zulassung und Kontrolle des Einsatzes von KI in Betracht. Dies ergibt sich bereits daraus, dass die Entscheidungsvorschläge von KI basierten Datenverarbeitungen in der Praxis bei den Entscheidern eine hohe Akzeptanz bis hin zur faktischen Bindung haben dürften, zumal sie diesen regelmäßig von rechtlichen Begründungslasten und -risiken freihalten.

Gerade in grundrechtssensiblen Bereichen wird daher auch hier eine Zulassungskontrolle für selbstlernende Systeme durch Daten verarbeitende Stellen erforderlich. Mit Blick auf die hohen Potentiale für Diskriminierungen von Personen ergeben sich auch für nicht selbstexekutive Entscheidungen besondere Risiken für die Grundrechte Betroffener.

Das ist der Fall, wenn die Gefahr besteht, dass Ergebnisse einer automatisierten Datenverarbeitung ohne eine eigenständige Überprüfung – quasi als Automatik – durch menschliche Entscheidungsträger übernommen werden. Gleiches gilt für Fälle, in denen die maschinelle Verarbeitung einen hohen Anteil an sog. false positives erzeugt und dadurch Rechte von Personen beeinträchtigt werden können, etwa bei einer automatisierten biometrischen Personenkontrolle in Echtzeit, die in der Praxis eine hohe Rate an Falschmeldungen und ggfs. vorläufigen Festnahmen bewirkt.

Gleiches gilt grundsätzlich für die Erzeugung von false negatives: Wenn Personen von einem System nicht erkannt werden, sind Grundrechtseingriffe in Form automatisierter Datenverarbeitungen für unbeteiligte Personen auch dann denkbar, wenn die eigentliche Entscheidung von Menschen getroffen wird. Das wäre etwa der Fall, wenn Roboter, deren Aufgabe darin besteht menschliches Leben nach Naturkatastrophen zu retten, menschliche Opfer nicht erkennen.

IV. Fazit

Eine ausschließlich auf das Innovationspotential von Künstlicher Intelligenz verengte Sichtweise widerspräche den Schutzpflichten des Staates gegenüber den digitalen Grundrechten der Bürgerinnen und Bürger. Selbstlernende Systeme sind, soweit sie in grundrechtssensiblen Bereichen eingesetzt werden, Risikotechnologien, deren Einsatz gerade im Bereich der öffentlichen Verwaltung enge Grenzen gezogen sind. Dies gilt in besonderer Weise, soweit dadurch automatische Entscheidungen ohne Zwischenschaltung menschlicher Entscheidungsträger umgesetzt werden sollen.

Der Einsatz von selbstlernenden Systemen in Staat und Verwaltung, die sich im Zuge des Einsatzes von automatisierten Entscheidungsverfahren ergeben, wirft verfassungsrechtliche sowie grundrechtliche Fragen auf. Hier finden sich insbesondere im Rahmen der DSGVO zahlreiche Vorgaben, die das Grundrecht auf informationelle Selbstbestimmung und den Schutz der Privatsphäre zum Gegenstand haben und den Rahmen abstecken, innerhalb dessen der Einsatz von Künstlicher Intelligenz als Risikotechnologie ausschließlich erfolgen darf.

Weitergehend ergeben sich aus Grundrechten bzw. grundrechtlichen Schutzpflichten verfassungsrechtliche Gewährleistungsgarantien für den Einsatz von selbstlernenden Systemen, die gerade aus deren Eigenart, unkontrollierbare und nicht vorhersehbare, letztlich sich einem gesetzlichen Zurechnungszusammenhang entziehende Eingriffe zu verursachen, resultieren. Der Schutz von Leben und Gesundheit, der Meinungsfreiheit und der Diskriminierungsfreiheit bei dem Einsatz von selbstlernenden Systemen ist zu beachten und führt zu Kontroll- und Überwachungsverfahren, die entsprechende Risiken minimieren.

Die höchste Eingriffsintensität geht von automatisierten Entscheidungen aus, die unmittelbar durch fortdauernd autonom lernende Systeme getroffen werden. Für die klassische Eingriffsverwaltung ergeben sich in diesem Bereich verfassungsrechtliche Hürden aus den Grundrechten und der rechtsstaatlichen Gesetzesbindung der

Verwaltung und dem Demokratieprinzip, die einen Einsatz durch Maschinen grundsätzlich nicht zulassen. Darunter fielen dann etwa autonome Waffensysteme zur Durchsetzung polizeilicher Anordnungen oder eine maschinelle Auswahl von Personen, die durch den Einsatz von KI als potentielle Störer der öffentlichen Sicherheit erkannt und den Ordnungsbehörden gemeldet werden.

Derartig enge Grenzen bestehen allerdings nicht bei Verfahren, in denen selbstlernende Systeme Entscheidungen lediglich vorbereiten. Hier ist nach wie vor eine menschliche Entscheidung maßgebend. Wenn es jedoch keine wirksamen Sicherungen dagegen gibt, dass die maschinellen Vorgaben in der Verwaltungspraxis durch menschliche Subjekte automatisch durchgesetzt werden, sind die Übergänge zu selbstexekutiven Maschinenentscheidungen nicht mehr relevant. Ein bloßes Nachvollziehen maschineller Entscheidungsvorschläge, die für die Betroffenen weder Ermessenserwägungen noch rational nachvollziehbare Begründungen liefern, lässt daher ebenfalls eine Bindung an gesetzliche Vorgaben vermissen. Damit fehlt es auch in diesen Fällen an einer Ableitbarkeit von Entscheidungen aus dem Gesetz. Das gilt allerdings nicht für deterministische algorithmische Entscheidungen, bei denen der Gesetzesvollzug durch den Algorithmus im Sinne eines Konditionalprogramms ohne die Möglichkeit eines maschinellen Entscheidungsspielraums abgebildet wird.

Soweit selbstlernende Systeme außerhalb der Eingriffsverwaltung betroffen sind, wie dies etwa beim vollautonomen Fahren der Fall ist, müssen die davon ausgehenden Risiken für die Verwirklichung von Grundrechten entsprechenden Zulassungs- und begleitenden Überprüfungsverfahren unterzogen werden. Es besteht eine Kontrollverantwortung durch unabhängige Stellen. Danach sind selbstlernende Systeme im Rahmen von Zulassungsentscheidungen und begleitenden Kontrollen durch unabhängige Stellen zu überprüfen. Es kommen hier gänzlich unterschiedliche Verfahren wie die Zertifizierung durch akkreditierte Stellen, aber auch durch staatliche Genehmigungsverfahren in Betracht.