

Innovation vs. Kontrollverlust? Ansätze der KI-Regulierung in der EU und China

Die rasante Entwicklung der Künstlichen Intelligenz („KI“) stellt Rechtsordnungen weltweit vor die Herausforderung, technologischen Fortschritt zu ermöglichen und zugleich Risiken für Grundrechte, Sicherheit und gesellschaftliche Ordnung wirksam zu begrenzen. Genau diesen Spagat versuchen sowohl die Europäische Union („EU“) als auch die Volksrepublik China („China“ oder „VR China“) mit einer Politik, die Innovation ermöglicht und zugleich eine regulierte KI-Entwicklung sicherstellen soll.

Der vorliegende Beitrag vergleicht die regulatorischen und datenschutzrechtlichen Rahmenbedingungen für KI in der EU und China. Im Zentrum stehen dabei generative KI-Systeme (z.B. Deepfakes), sowie algorithmische Empfehlungssysteme, die exemplarisch die Ambivalenz zwischen Innovationsfortschritt und Kontrollbedarf verdeutlichen. Untersucht wird, wie beide Rechtsordnungen versuchen, dieses Spannungsverhältnis aufzulösen und welche Konsequenzen sich daraus für Transparenz, Verantwortlichkeit und Innovationsfreiheit ergeben.

I. Regulatorische Grundlagen in der EU

Die europäische KI-Regulierung verfolgt einen **menschenzentrierten und grundrechtsorientierten Ansatz**¹, der individuelle Rechte, Verbraucherschutz und die Wahrung des Binnenmarkts miteinander verbindet. Anstelle eines einheitlichen KI-Gesetzes stützt sich der europäische Rechtsrahmen auf ein **mehrschichtiges Zusammenspiel mehrerer Verordnungen**: die Datenschutz-Grundverordnung („DSGVO“)² als horizontaler Datenschutzrahmen, der Digital Services Act („DSA“)³ zur Regulierung digitaler Plattformstrukturen und die Verordnung (EU) 2024/1689 über KI („KI-VO“)⁴ als spezialgesetzliches Instrument zur risikobasierten Regulierung von KI-Systemen. Diese Rechtsakte greifen **systematisch ineinander** und schaffen gemeinsam ein kohärentes Regelwerk, das technologische Innovation fördert und gleichzeitig Grundrechte schützt.

1. Datenschutzrechtlicher Ausgangspunkt: Die DSGVO

Die DSGVO bildet das datenschutzrechtliche Fundament für die KI-Anwendung in der EU. Zwar erwähnt sie „Künstliche Intelligenz“ nicht ausdrücklich, ihre Vorgaben – insbesondere Datenminimierung, Zweckbindung, Transparenz und „Privacy by Design“ – gelten technologieagnostisch auch für KI-Systeme. Besondere Bedeutung hat in diesem Zusammenhang Art. 22 DSGVO: Betroffene dürfen grundsätzlich keiner ausschließlich

¹ <https://www.consilium.europa.eu/en/press/press-releases/2025/05/23/council-calls-for-an-inclusive-ethical-sustainable-and-human-centric-strategy-for-the-uptake-of-ai-in-science/>; https://www.edps.europa.eu/press-publications/press-news/blog/global-and-collective-effort-embrace-technologies-human-centric-way_en.

² Datenschutzgrundverordnung: <https://dsgvo-gesetz.de>.

³ Digital Services Act: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32022R2065>.

⁴ KI-VO: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1689>.

automatisierten Entscheidung, einschließlich „Profiling“, unterworfen werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Im Kontext der DSGVO ist „Profiling“ jede automatisierte Verarbeitung personenbezogener Daten, um persönliche Aspekte einer natürlichen Person zu bewerten, bestimmte Eigenschaften zu analysieren oder zukünftiges Verhalten vorherzusagen.⁵ Das „Profiling“ kann – je nach Zweck – auch auf anderer Rechtsgrundlage erfolgen (z.B. Art. 6 Abs. 1 lit. b/f DSGVO). Art. 22 greift nur, wenn die Entscheidung *ausschließlich automatisiert* erfolgt und rechtliche oder vergleichbare Wirkung entfaltet. Ausnahmen vom Verbot der automatisierten Einzelfallentscheidungen bestehen nur bei ausdrücklicher Einwilligung, gesetzlicher Ermächtigung oder Erforderlichkeit für einen Vertrag; auch dann sind Schutzmechanismen wie menschliches Eingreifen, transparente Information und eine nachvollziehbare Erläuterung der zugrunde liegenden Logik sicherzustellen. Neben diesem zweistufigen Ansatz (Profiling + automatisierte Entscheidungsfindung) statuieren Artikel 5 Abs. 1 lit. a und Art. 13–14 DSGVO umfassende Informations- und Transparenzpflichten. Bei risikoreichen Verarbeitungen, typischerweise bei umfangreichem Profiling, ist eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen.

2. Plattformregulierung und algorithmische Transparenz: Der Digital Services Act (DSA)

Neben dem Datenschutz adressiert der DSA Dienste- und Plattformrisiken. Für Online-Plattformen schreibt Art. 27 DSA vor, die wichtigsten Parameter ihrer Empfehlungsalgorithmen in den AGB offenzulegen. Für sehr große Online-Plattformen und Suchmaschinen (VLOPs/VLOSEs)⁶ gilt zusätzlich Art. 38 DSA: Mindestens eine Empfehlungsoption muss ohne „Profiling“ bereitgestellt werden. Darüber hinaus müssen VLOPs ihre systemischen Risiken regelmäßig bewerten (Art. 34 DSA) und geeignete Risikominderungsmaßnahmen ergreifen (Art. 35 DSA) – dies gilt auch für Risiken, die aus dem Einsatz algorithmischer Systeme resultieren (z.B. Verbreitung illegaler Inhalte, Beeinträchtigung von Grundrechten, Desinformation). In der Praxis greifen DSGVO und DSA ineinander: Während die DSGVO die Verarbeitung personenbezogener Daten schützt, adressiert der DSA die Funktionsweise und Wirkung algorithmischer Systeme in der digitalen Öffentlichkeit.

3. Die KI-VO: Horizontale Regulierung nach Risikostufen

Den Kern der europäischen KI-Regulierung bildet die KI-VO. Sie wurde am 13. Juni 2024 erlassen und ist am 1. August 2024 in Kraft getreten; die materiellen Pflichten in Kapitel I und II (Verbotene Praktiken) gelten seit dem 2. Februar 2025. Die Vorschriften zu General Purpose AI („GPAI“) gelten seit dem 2. August 2025 und die Vorschriften für Hochrisiko-KI sollen ab dem 2. August 2026 in Kraft treten, wobei eine Frist an die Verfügbarkeit von technischen Standards gekoppelt werden soll, spätestens jedoch am 2. Dezember 2027 für Hochrisiko-KI nach Anhang III (bspw. Systeme in den Bereichen Kreditwürdigkeit) bzw. 2. August 2028 für Hochrisiko-KI nach Anhang I (bspw. für produktsicherheitsrelevante Komponenten).

⁵ Definition „Profiling“ nach Art. 4 Abs. 4 DSGVO: <https://dsgvo-gesetz.de/art-4-dsgvo/>.

⁶ Definition der Europäischen Kommission zu Very Large Online Platforms: <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>.

Die KI-VO baut als *lex specialis* auf den bestehenden Datenschutz- und Plattformregeln auf und verknüpft Marktregulierung mit Grundrechtsschutz (primär gestützt auf Art. 114 AEUV⁷). Die KI-VO ergänzt komplementär die DSGVO (Datenverarbeitung) und den DSA (Platformaufsicht) durch produkt- und technikbezogene Marktregeln. Die KI-VO folgt einem risikobasierten Ansatz: Je höher das Risiko, das von einem KI-System ausgeht, desto strenger sind die rechtlichen Anforderungen.⁸

- **Unacceptable Risk (Art. 5 KI-VO):** Verbot u.a. manipulativer Praktiken, Ausbeutung schutzbedürftiger Gruppen, staatlichen Social Scorings, ungezielten Scrapings biometrischer Daten zur Gesichtserkennung sowie Emotionserkennung in Arbeit und Bildung; biometrische Fernidentifikation im öffentlichen Raum ist weitgehend untersagt; nur eng begrenzte gesetzliche Ausnahmen. Diese Verbote spiegeln zentrale ethische Leitprinzipien der EU wider.⁹
- **High Risk:** Für Hochrisiko-KI (u.a. in kritischer Infrastruktur, Bildung/Beschäftigung, Kredit- und Gesundheitswesen, Strafverfolgung/Migration) gelten detaillierte Pflichten: Risikomanagement (Art. 9), Daten- und Daten-Governance (Art. 10), technische Dokumentation (Art. 11), Record-Keeping/Logging (Art. 12), Transparenz und Information für Nutzer (Art. 13), menschliche Aufsicht (Art. 14) sowie Genauigkeit/Robustheit/Cybersicherheit (Art. 15). Je nach Verfahren ist eine Konformitätsbewertung – teils durch eine benannte Stelle – erforderlich (Art. 43).
- **Limited Risk:** Für bestimmte Systeme (z.B. Interaktions-KI, Emotionserkennung, biometrische Kategorisierung sowie Systeme zur synthetischen Inhaltserzeugung/“Deepfakes“) gelten Transparenz- und Kennzeichnungspflichten (Art. 50). Nutzer müssen erkennen können, dass sie mit KI interagieren bzw. dass Inhalte künstlich erzeugt oder manipuliert wurden.
- **Minimal Risk:** Für die Mehrheit der KI-Anwendungen (etwa Spam-Filter oder rein nicht-personenbezogene Optimierungen) greifen keine zusätzlichen Pflichten.

Ergänzend fördert die KI-VO Innovation – etwa durch sog. *Regulatory Sandboxes* – und etabliert ein EU-KI-Büro zur Koordinierung der Aufsicht. Die KI-spezifischen Pflichten gelten neben der DSGVO und lassen deren Anforderungen unberührt; ebenso bleiben DSA-spezifische Plattformpflichten bestehen.

Ausblick bis 2030: Die EU plant, KI-VO in den kommenden Jahren dynamisch weiterzuentwickeln und mit parallellaufenden Digitalgesetzen wie dem Data Act¹⁰ und dem DSA zu verzahnen. Geplant sind regelmäßige Überprüfungen der Risikoklassifizierung sowie mögliche Anpassungen für Basis-/Allzweckmodelle. Bis 2030 soll ein kohärenter europäischer KI-Governance-Rahmen entstehen, der technische Standards, Aufsichtsstrukturen und Haftungsfragen stärker integriert.

II. Regulatorische Grundlagen in China

⁷ Vertrag über die Arbeitsweise der EU: <https://dejure.org/gesetze/AEUV/114.html>.

⁸ Ausführungen der Europäischen Kommission zu den KI-Risikoklassen: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#:~:text=All%20AI%20systems%20considered%20a,Act%20prohibits%20eight%20practices%2C%20namely.>

⁹ <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act.> (Download Link klicken).

¹⁰ Data Act: <https://eur-lex.europa.eu/eli/reg/2023/2854.>

China verfolgt das Ziel, die Entwicklung von KI zu fördern und gleichzeitig Risiken zu begrenzen aus einer anderen Perspektive als die EU. Die chinesische Regierung betrachtet KI als Schlüsseltechnologie für zukünftige marktwirtschaftliche Stärke Chinas. KI wurde in dem am 12. März 2026 verabschiedeten 15. Fünfjahresplan (2026 bis 2030) zusammen mit sieben weiteren Technologien als „Zukunftstechnologie“ eingestuft. Dabei setzt China auf die Entwicklung und Nutzung von KI-Technologien unter Gewährleistung der nationalen Sicherheit, der Einhaltung ethischer Standards und gesellschaftlicher Werte Chinas.

Chinas Gesetzgebung im Bereich KI folgt einem stufenweisen Prozess: Ausgangspunkt waren allgemeine Strategien und Entwicklungsziele, die sich sukzessive in sektor- und anwendungsspezifische Vorschriften verdichteten. Dabei verschob sich der Fokus von reiner Wachstumsförderung zu einem ausgewogenen Verhältnis von Innovation und Risikosteuerung, bis schließlich ein ganzheitliches, systematisches Regelwerk entstehen soll.

In China gibt es zum Datum der Veröffentlichung dieses Artikels (noch) kein umfassendes KI-Gesetz. Stattdessen beruht der KI-Rechtsrahmen auf politischen Zielvorgaben sowie einer Kombination aus allgemeinen Gesetzen, Verordnungen, Leitlinien und technischen Standards, die auch für KI-Anwendungen relevant sind. Im Folgenden werden die zentralen Gesetze skizziert.

1. Datenschutz und automatisierte Entscheidungen: Das GSPD

Mit dem Gesetz zum Schutz personenbezogener Daten („GSPD“) ¹¹ (engl. Personal Information Protection Law oder „PIPL“) von 2021 hat China erstmals ein umfassendes Datenschutzgesetz erlassen, das in vielerlei Hinsicht Ähnlichkeiten mit der DSGVO aufweist und indirekt Anwendung auf KI-Anwendungen findet:

Nach dem GSPD müssen KI-Anbieter als Verarbeiter personenbezogener Daten u.a. die Prinzipien der Rechtmäßigkeit und Zweckbindung beachten, einen Datenschutzbeauftragten in China benennen und verarbeitete personenbezogene Daten grundsätzlich in China speichern. Personenbezogene Daten dürfen nur nach Erfüllung zusätzlicher Auflagen ins Ausland übermittelt werden. Sie müssen die Betroffenen - also die Nutzer - über Verarbeitungszweck, Speicherdauer und ihre Rechte (Auskunft, Berichtigung, Löschung) informieren.

Besondere Bedeutung hat Art. 24 GSPD, der sich ausdrücklich mit automatisierten Entscheidungsprozessen befasst (vergleichbar mit Art. 22 DSGVO). Art. 24 GSPD bestimmt, dass Unternehmen bei automatisierten Entscheidungen Transparenz, Fairness und Unparteilichkeit sicherstellen müssen. Wird eine Entscheidung mittels KI getroffen, die wesentliche Auswirkungen auf Rechte und Interessen einer Person hat, steht dieser Person ein Recht auf Erläuterung der Entscheidung und das Recht zu verlangen, dass die Entscheidung nicht ausschließlich durch Algorithmen gefällt wird. Darüber hinaus verlangt Art. 55 GSPD vor allem bei umfangreicher automatisierter Datenverarbeitung die Durchführung von

¹¹ 中华人民共和国个人信息保护法: https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm

Datenschutz-Folgenabschätzungen (engl. Personal Information Protection Impact Assessment oder „PIPIA“) und eine Aufzeichnung der Verarbeitungsaktivitäten.¹²

2. Regulierung von Algorithmus-Empfehlungen und KI-Kennzeichnung

Nach der Festlegung des für die Regulierung von KI notwendigen Datenschutz-, Daten- und Cybersicherheitsrechtsrahmens – bestehend u.a. aus dem GSPD, dem Cybersicherheitsgesetz und dem Datensicherheitsgesetz – im Jahr 2021 wurden in China die ersten direkten sektorspezifischen KI-Regulierungen mit dem Fokus auf Behebung einiger KI-spezifischen Risiken erlassen.

Zwei zentrale und rechtsverbindliche KI-Regelungen sind die Bestimmungen über Empfehlungsalgorithmen in internetbasierten Informationsdiensten („Bestimmungen über Algorithmus-Empfehlungen“),¹³ und die Bestimmungen über Tiefensynthese für Internet-Informationendienste („Deep-Synthesis-Bestimmungen“)¹⁴, die von der Cyberspace Administration of China („CAC“) erlassen wurden und am 1. März 2022 bzw. am 10. Januar 2023 in Kraft getreten sind.

Die **Bestimmungen über Algorithmus-Empfehlungen** richten sich an Anbieter von Internetdiensten, die Algorithmen für personalisierte Empfehlungen einsetzen (z.B. Social-Media-Feeds, E-Commerce-Vorschläge), also beispielsweise soziale Netzwerke, E-Commerce-Plattformen mit „Das gefällt dir vielleicht“-Funktion, Ride-hailing-Apps oder Suchmaschinen.

Die Bestimmungen über Algorithmus-Empfehlungen umfassen folgende Kernanforderungen für Anbieter von Internetdiensten:

- **Inhaltliche Vorgaben:** Die Verwendung von Algorithmen zur Erstellung von „illegalen Inhalten“ ist verboten. „Illegal“ bezieht sich auf gesetzlich verbotene Inhalte, die z.B. die nationale Sicherheit, die sozialistische Ordnung oder die legitimen Rechte und Interessen Dritter gefährden (Art. 6). Es ist weiterhin verboten, Algorithmen einzusetzen, um die Nutzer zur Sucht oder zum übermäßigen Konsum zu verleiten (Art. 8).
- **Prüfung- und Offenlegungspflicht:** Anbieter müssen die Algorithmen und Anwendungsergebnisse regelmäßig auditieren (Art. 8). Sie müssen die Nutzer „in auffälliger Weise“ über den Einsatz von Empfehlungsalgorithmen informieren und Grundprinzipien, Zweck sowie Funktionsabläufe des Algorithmus veröffentlichen (Art. 16).
- **Nutzerrechte:** Anbieter müssen den Nutzern die Option anbieten, zu „neutralen“ Inhalten, die nicht auf deren individuelle Merkmale zugeschnitten sind, umzustellen, oder personalisierte Empfehlungen zu deaktivieren. Die Nutzer müssen zudem die Option haben, die Nutzer-Tags, die in ihren Nutzerprofilen vermerkt sind, einzusehen und zu löschen (Art. 17).

¹² Für mehr Informationen zum Vergleich zwischen der DSGVO und dem GSPD siehe Artikel „Das neue chinesische Datenschutzrecht und die europäische DSGVO im Rechtsvergleich“, abrufbar unter https://bktlegal.com/wp-content/uploads/2024/11/20211210_BKT_DSB_12_2021_Beitrag_Burkardt_Recha.pdf

¹³ 互联网信息服务算法推荐管理规定: https://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm.

¹⁴ 互联网信息服务深度合成管理规定: https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm

- **Verbot diskriminierender Praktiken:** So wie Art. 24 GSPD bereits Preisdiskriminierung verbietet, verbieten die Bestimmungen in Art. 21 ebenso ausdrücklich unrechtmäßige Preisdifferenzierung basierend auf Nutzerprofilen.
- **Sicherheits- und Ethikprüfungen:** Anbieter müssen Informationssicherheit verstärken, und ein System zur Erkennung und Löschung rechtswidriger und schädlicher Inhalte aufbauen bzw. verbessern (Art. 9).
- **Algorithmen-Registrierung:** Anbieter von KI-Diensten, die über „öffentliche Meinungsbildung oder gesellschaftliches Mobilisierungspotenzial“ verfügen (etwa große Social-Media- und News-Plattformen), müssen Informationen zu eingesetzten Algorithmen, ein Selbstbewertungsbericht sowie andere Informationen bei den Behörden registrieren (Art. 24).¹⁵

Neben den Bedenken gegen algorithmische Empfehlungen rückte die Bedrohung durch „Deepfakes“ in den Fokus der chinesischen Regierung. Aufgrund der täuschend echten Videos oder Audios, die Falschinformationen verbreiten und häufig unbefugte Gesichtssynthesen zeigen, intensivierte China die Kontrolle über KI-generierte Inhalte und hat hierzu die **Deep-Synthesis-Bestimmungen** erlassen.

„Deep Synthesis“ nach den Deep-Synthesis-Bestimmungen bezeichnet KI-gestützte Erzeugung von Text, Bildern, Audio, Video etc. Die Deep-Synthesis-Bestimmungen enthalten eine umfassende Reihe von Pflichten für Anbieter von Deep-Synthesis-Dienstleistungen, wie z.B.:

- **Verbot bestimmter Inhalte:** So wie in den Bestimmungen über Algorithmus-Empfehlungen, ist auch hier jegliche gesetzwidrige, „staatsschädigende“ oder die öffentliche Ordnung gefährdende Verwendung von KI sowie Erstellung von gefälschten Nachrichten verboten (Art. 6).
- **Informationssicherheitspflichten:** Auch nach den Deep-Synthesis-Bestimmungen haften Anbieter für die Informationssicherheit und müssen ein umfassendes System aufbauen, das u. a. Nutzerregistrierung, Audits der Algorithmen, Ethik-Reviews, Inhaltsmoderation, Datenschutz, Anti-Betrug und Notfallpläne umfasst (Art. 7).
- **Kennzeichnungspflicht:** Alle KI-generierten Inhalte müssen deutlich als solche gekennzeichnet sein, insbesondere Deepfake-Formate wie z.B. Stimmenimitationen, synthetische Dialoge oder Gesichtssynthesen. Die Kennzeichnungen dürfen nicht gelöscht werden (Art. 16-18).
- **Überwachungspflichten:** Anbieter sind verpflichtet, ein solides Gerüchtebekämpfungssystem aufzubauen. Sobald sie feststellen, dass über die von ihnen angebotenen Deep-Synthesis-Dienste falsche Informationen erstellt, vervielfältigt, veröffentlicht oder verbreitet werden, sind sie verpflichtet, unverzüglich geeignete Gegenmaßnahmen zu ergreifen und einen Bericht bei der CAC einzureichen (Art. 11).

Ergänzend hat die CAC am 7. März 2025 spezielle Bestimmungen zur Kennzeichnung der durch KI erzeugte und zusammengesetzte Inhalte¹⁶ veröffentlicht. Diese sind am 1. September 2025

¹⁵ Nach der Ankündigung der CAC wurden zum 31. März 2025 bei der CAC insgesamt 346 generative KI-Dienste registriert: http://english.scio.gov.cn/pressroom/2025-04/09/content_117814020.html

¹⁶ 人工智能生成合成内容标识办法: https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm

in Kraft getreten und enthalten eine spezifische Anleitung, wo und wie KI-generierte Inhalte sichtbar und unsichtbar gekennzeichnet werden müssen.

3. Regelungen zum Management von generativer KI

Am 10. Juli 2023 sind die Interimsmaßnahmen für das Management von generativer KI („KI-Maßnahmen“)¹⁷ erlassen worden und am 15. August 2023 in Kraft getreten, die eine "umfassende und umsichtige, kategorisierte und klassifizierte" Regulierung von generativen KI-Diensten zum Ziel haben. Die KI-Maßnahmen richten sich spezifisch an KI-Anbieter, die „der Öffentlichkeit in China generative Text-, Bild-, Audio- oder Videodienste anbieten“ („öffentliche KI-Dienstanbieter“). Die zentralen Vorgaben lassen sich wie folgt zusammenfassen:

- **Verantwortung für generierte Inhalte:** Anbieter müssen sicherstellen, dass die generierten Inhalte mit den Gesetzen, den sozialistischen Werten, der sozialen Moral und der öffentlichen Ordnung übereinstimmen. Insbesondere ist die Schaffung von Fehlinformationen, Anstiftung zum Sturz des sozialistischen Systems, Gefährdung der nationalen Sicherheit und Interessen untersagt (Art. 4).
- **Legale Datenquellen und IP-Schutz:** Die Anbieter müssen Daten und grundlegende Modelle aus legalen Quellen verwenden, die Rechte am geistigen Eigentum anderer beachten und Geschäftsgeheimnisse wahren (Art. 9).
- **Kennzeichnung und Transparenz:** Ähnlich den Deep Synthesis-Bestimmungen fordern die KI-Maßnahmen, dass generierte Inhalte markiert werden (Art. 12).
- **Offenlegungspflichten ggü. Behörden:** Die Anbieter müssen der CAC auf Anforderung Informationen zu den eingesetzten Datenquellen, deren Umfang, den verwendeten Kennzeichnungsregeln und zu den grundlegenden Algorithmen zur Verfügung stellen (Art. 19).

Ausblick: Am 26. Juli 2025 veröffentlichte China auf der World Artificial Intelligence Conference 2025 seinen AI Action Plan¹⁸, nach dem grenzüberschreitende Innovation, Open-Source- und Datenteilung unter hohen Sicherheits-, Datenschutz- und Diversitätsstandards, etabliert werden, und Forschungsergebnisse in konkrete Anwendungen in Industrie, Gesundheit, Bildung und Smart Cities umgewandelt werden sollen.

Die am 26. August 2025 veröffentlichte Umsetzungsrichtlinie zur Initiative AI Plus¹⁹ setzt weitere ehrgeizige Ziele für die Implementierung von KI: Bis 2027 soll China eine führende Rolle bei der umfassenden und tiefgreifenden Integration von KI in sechs Schlüsselbranchen einnehmen. Eine Verbreitungsrate von intelligenten Endgeräten und KI-Agenten der neuen Generation soll bis 2027: 70% und bis 2030: 90% überschreiten.

Angesichts der vorstehenden Ziele zur Implementierung von KI ist mit einem Erlass von weiteren KI-Regeln zu rechnen. Nach dem Gesetzgebungsplan des Staatsrats von 2023²⁰ sollen

¹⁷ 生成式人工智能服务管理暂行办法: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm.

¹⁸ 人工智能全球治理行动计划: https://www.mfa.gov.cn/web/zyxw/202507/t20250726_11677803.shtml

¹⁹ 国务院关于深入实施“人工智能+”行动的意见: https://www.mee.gov.cn/zcwj/gwywj/202508/t20250827_1126207.shtml

²⁰ Gesetzgebungsplan des Staatsrates von 2023: https://www.gov.cn/zhengce/content/202306/content_6884925.htm

ein umfassendes KI-Gesetz sowie 50 zusätzliche nationale und branchenspezifische Standards in 2026 verabschiedet werden.²¹

So haben z.B. die Staatsverwaltung für Marktaufsicht (SAMR) und die Nationale Standardisierungsbehörde am 25. April 2025 gemeinsam drei nationale Standards zur Stärkung der Sicherheit und Governance generativer KI veröffentlicht, die am 1. November 2025 in Kraft getreten sind.²² Darüber hinaus hat die Nationale Normungsrichtlinie der Technischen Kommission für Informationssicherheit (TC260) am 15. September 2025 den revidierten KI-Sicherheits-Governance-Rahmen²³ erlassen, welcher eine auf Risikomanagement gestützte Governance-Methodik vorsieht und teilt KI-Sicherheitsrisiken in drei Hauptkategorien: technisch-endogene Sicherheitsrisiken (z. B. Algorithmen-Bias, Modellfehler), technisch-anwendungsbezogene Sicherheitsrisiken (z. B. Cyber-Angriffe, Content-Sicherheit) sowie anwendungs-derivierte Sicherheitsrisiken (z. B. ethische und gesellschaftliche Auswirkungen). Auf Basis der Risikoklassifizierung sind die Risiken zu bewerten und entsprechende Maßnahmen zu ergreifen.

4. Sonderregelungen und Sandbox-Ansätze

Die VR China verfügt bislang über kein nationales KI-Sandbox-Rahmenwerk. In China sollen die sog. „KI-Sandboxes“ von Pilotstädten wie Shanghai und Shenzhen umgesetzt werden. So steht es z.B. in der Verordnung zur Förderung der Entwicklung der Künstlichen-Intelligenz-Industrie in der Stadt Shanghai²⁴, dass die Behörden entsprechende Aufsichts-, Regel- und Standardvorschriften erlassen, gestufte Steuerung und Sandbox-Regulierung erproben, die Innovationskraft aller Akteure anregen und den Entwicklungsspielraum der KI erweitern sollen.

Im Vergleich dazu stehen die europäischen KI-Sandboxes auf dem Fundament der EU-KI-Verordnung (Art. 53-57): Vorgesehen sind unionsweit koordinierte Sandbox-Verfahren mit befristeter Teilnahme und strukturierter behördlicher Begleitung, einschließlich Risiko- und Ethikbewertungen.

Während Shanghai und Shenzhen regulatorische Flexibilität durch lokale Erlasse erzeugen, nutzt Europa ein zentrales, längerfristig standardisiertes Verfahren – mit dem Vorteil grenzüberschreitender Gültigkeit, aber mit vergleichsweise aufwendigen Prüf- und Abstimmungsprozessen.

III. Fallbeispiele im Rechtsvergleich

Um die praktische Wirkung der zuvor dargestellten Regelungen zu verdeutlichen, werden im Folgenden zwei exemplarische Anwendungsszenarien betrachtet.

²¹ Leitlinien für den Aufbau eines umfassenden Normungssystems für die nationale Industrie der künstlichen Intelligenz von 2024: <https://www.gov.cn/zhengce/zhengceku/202407/P020240702716282797987.pdf>

²² „Cybersicherheitstechnik – Sicherheitsanforderungen an die Datenannotation generativer KI“, „Cybersicherheitstechnik – Sicherheitsanforderungen an Vor-Training und Feinabstimmungsdaten generativer KI“, und „Cybersicherheitstechnik – Grundlegende Sicherheitsanforderungen an Dienste generativer KI“.

²³ 《人工智能安全治理框架》2.0 : https://www.cac.gov.cn/2025-09/15/c_1759653448369123.htm

²⁴ 《上海市促进人工智能产业发展条例》, http://www.legaldaily.com.cn/Company/content/2022-09/27/content_8785718.html

1. E-Commerce-Empfehlungssysteme

EU: Ein Online-Händler, der personalisierte Produktempfehlungen anbietet, muss die Vorgaben der DSGVO (Art. 6,22) beachten. Die Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage nach Art. 6 DSGVO. Profiling kann je nach Kontext auf unterschiedliche Erlaubnistatbestände gestützt werden; Art. 22 DSGVO greift jedoch nur bei ausschließlich automatisierten Entscheidungen, die gegenüber der betroffenen Person rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen. In diesen Fällen sind insbesondere angemessene Schutzmaßnahmen wie das Recht auf menschliches Eingreifen, auf Darlegung der Entscheidungslogik und auf Anfechtung der Entscheidung sicherzustellen. Große Plattformen unterliegen zusätzlich dem DSA: Sie müssen die wesentlichen Parameter ihrer Empfehlungssysteme offenlegen (Art. 27 DSA) und Nutzern mindestens eine nicht auf Profiling beruhende Empfehlungsmöglichkeit anbieten (Art. 38 DSA). Insgesamt haben Anbieter in der EU weitgehend viel Freiheit in der Ausgestaltung, solange datenschutzrechtliche Transparenz- und Rechtmäßigkeitsanforderungen eingehalten werden. Eine vorab behördliche Genehmigung ist in der Regel nicht nötig; vielmehr greifen später Datenschutzkontrollen und mögliche Datenschutz-Folgenabschätzungen.

China: Der Betreiber eines Online-Shops bzw. einer E-Commerce Plattform in China muss außer der Beachtung allgemeiner datenschutzrechtlicher Pflichten nach dem GSPD seine Nutzer darüber informieren, dass ein Empfehlungsalgorithmus eingesetzt wird. Der Betreiber muss Informationen über den Empfehlungs-Algorithmus offenlegen und, sollten dem Nutzer auf Basis automatisierter Entscheidungsfindung erstellte Informationen zugestellt werden – wie z.B. Werbung, Produktempfehlungen –, eine „Opt-out“ Option zur Verfügung stellen, bzw. eine Option, diese Funktion zu „de-individualisieren“ oder auszuschalten.

Sollte ein KI-System für die Preisgestaltung verwendet werden, unterliegt dies besonderen Anforderungen: Es ist untersagt, aufgrund von Präferenzen, Handelsgewohnheiten oder anderen Merkmalen der Konsumenten unangemessene Unterschiede in den Handelsbedingungen – insbesondere in den Preisen – vorzunehmen.

Bei möglichen unerwünschten Inhalten in Empfehlungen – etwa, wenn Produkte mit „negativen“ Inhalten verknüpft werden – haftet der Plattformbetreiber unmittelbar. So würde z.B. eine Empfehlung des Algorithmus, ein T-Shirt mit dem Aufdruck „1989 – Never Forget“ – welches an die Proteste auf dem Tiananmen-Platz in 1989 erinnert – zu kaufen als **illegale Informationsverbreitung eingestuft**.

Der Betreiber muss sein Empfehlungssystem-Algorithmus bei der CAC nur dann registrieren, wenn Nutzer in dem Onlineshop **Meinungen äußern oder zu Aktionen aufgerufen werden können** (Foren, Bewertungen mit Like/Share/Streaming, Ranglisten, Influencer-Lives usw.).

2. Generativer KI-Chatbot

EU: Generative KI-Chatbots dürfen grundsätzlich auf den Markt gebracht werden. Vor 2024 gab es keine spezifischen Regelungen für den Umgang mit generativer KI, doch mit Inkrafttreten des AI-Act gelten klare Vorgaben. Chatbots dürfen in der Regel als Systeme mit „begrenztem Risiko“ eingestuft werden. Für generative KI sind Transparenzpflichten für

konkrete Systeme von modellbezogenen Pflichten für General-Purpose-AI-Modelle zu unterscheiden. Anbieter müssen dabei je nach Einordnung insbesondere Transparenzanforderungen beachten. Werden personenbezogene Daten verarbeitet, gelten die DSGVO-Vorschriften ergänzend. Werden für Entwicklung, Training oder Nutzung generativer KI personenbezogene Daten verarbeitet, richtet sich die Zulässigkeit nach den allgemeinen Vorgaben der DSGVO; eine Einwilligung ist dabei nicht in jedem Fall zwingend.

Treffen Chatbots autonome Entscheidungen mit rechtlicher Wirkung (z.B. Vertragsabschlüsse), greift zusätzlich Art. 22 DSGVO. Eine Zulassungspflicht besteht nicht, wohl aber die Pflicht zu sorgfältiger interner Compliance.

China: Wenn ein KI-Chatbot (wie z.B. DeepSeek) in China der Öffentlichkeit angeboten wird, muss der Anbieter sowohl die allgemeinen chinesischen Cybersicherheits- und Datenschutzvorschriften als auch die speziellen Regeln für generative KI-Dienste erfüllen:

Da generative KI-Chatbots als „Internet-Content-Service“ gelten, ist eine ICP-Registrierung erforderlich. Vor dem Inbetriebnehmen des Chatbots muss der Anbieter – wie oben erwähnt – bei der CAC ein Sicherheits-Self-Assessment einreichen und den Algorithmus registrieren. Darüber hinaus ist eine Sicherheitsbeurteilung nach der Verordnung über Internet-Informationssicherheit²⁵ erforderlich.

Der Anbieter muss die Trainingsdaten streng kontrollieren: Illegale, diskriminierende oder unangemessene Inhalte sind verboten. Der Anbieter muss sicherstellen, dass die durch den KI-Chatbot generierten Inhalte laufend überwacht und moderiert werden. Dies ergibt sich aus mehreren geltenden Vorschriften, einschließlich der KI-Maßnahmen. So dürfen z.B. politisch „heikle“ Themen nicht behandelt werden. Jede Antwort bzw. andere generierten Inhalte des KI-Chatbots müssen deutlich als „KI-generiert“ gekennzeichnet werden.

IV. Fazit

Die EU verfolgt bei der Regulierung von KI einen risikobasierten Ansatz, der Grundrechte, den Schutz der Privatsphäre und die individuelle Freiheit der Nutzer in den Mittelpunkt stellt. Der Rechtsrahmen aus DSGVO, DSA und AI-Act ist stark grundrechtsorientiert und setzt auf Transparenz, individuelle Entscheidungsfreiheit sowie den Schutz vor Diskriminierung. Innovation wird gezielt gefördert – etwa durch regulatorische Sandboxes –, steht jedoch stets im Spannungsfeld einer anspruchsvollen Compliance.

China hingegen orientiert sich an einem staatszentrierten Modell. KI-Entwicklung soll ausdrücklich den wirtschaftlichen und gesellschaftspolitischen Zielen dienen: Soziales Gleichgewicht und die Überwachung des öffentlichen Diskurses haben Vorrang. Gleichzeitig fließen immense Mittel in Forschung, Aufbau von KI und KI-Ökosystemen.

Beide Ansätze zielen darauf ab, Risiken zu minimieren und Innovation zu ermöglichen, unterscheiden sich jedoch grundlegend in ihrer Ausrichtung. In der EU steht der Schutz des

²⁵ 具有舆论属性或社会动员能力的互联网信息服务安全评估规定: https://www.gov.cn/zhengce/zhengceku/2018-11/30/content_5457763.htm

Individuums im Vordergrund: Der Mensch soll Herr des Algorithmus bleiben. China denkt vom Schutz des Staats her: Der Staat muss die Inhalte steuern, um gesellschaftspolitische Ziele durchzusetzen. Der zukünftige Wettbewerb wird daher nicht nur technologisch entschieden, sondern auch durch die Frage, welcher Rechtsrahmen Innovation unter Wahrung zentraler Werte besser ermöglicht.

Aktuell gelten die chinesischen KI-Regelungen primär für öffentlich angebotene KI-Dienste. Unternehmensinterne Entwicklungen oder Anwendungen generativer KI sind nicht explizit erfasst, unterliegen jedoch weiterhin allgemeinen gesetzlichen Vorgaben, insbesondere im Datenschutz-, Produkthaftungs-, Urheber- und Verbraucherschutzrecht. Angesichts der rasanten KI-Entwicklung ist damit zu rechnen, dass bald auch spezielle KI-Regelungen für unternehmensinterne KI-Anwendung erlassen werden. Wenn Sie unser Mandantenrundsreiben schon erhalten haben, informieren wir Sie in unregelmäßigen Abständen über die gesetzliche Entwicklung. Sollten Sie darüber hinaus Fragen oder Anmerkungen haben, so sprechen Sie uns gerne jederzeit an!

Ihr Burkardt & Partner Team



BURKARDT & PARTNER RECHTSANWÄLTE

Suite 1706, Five Corporate Avenue, No. 150 Hubin Road, Shanghai 200021, P.R. China

E-MAIL info@bktlegal.com

WEBSITE www.BKTlegal.com

OFFICE +86 (21) 6321 0088

Connect with us on [LinkedIn](#)