

Bayerisches Staatsministerium des Innern, für Sport und Integration



Bayerisches Staatsministerium des Innern, für Sport und Integration
80524 München

Präsidentin
des Bayer. Landtags
Frau Ilse Aigner, MdL
Maximilianeum
81627 München

Ihr Zeichen, Ihre Nachricht vom
P I-1312-3-5/201 I
16.10.2025

Unser Zeichen
C13-0016-1-VeCR

München
19.12.2025

Schriftliche Anfrage der Abgeordneten Florian von Brunn und Christiane Feichtmeier vom 16.10.2025 betreffend Straftaten, Diskriminierung und Sicherheitsvorfälle durch Künstliche Intelligenz in Bayern: Erfassung, Strafverfolgung und Prävention

Sehr geehrte Frau Landtagspräsidentin,

die Schriftliche Anfrage beantworte ich im Einvernehmen mit dem Staatsministerium für Wohnen, Bau und Verkehr, dem Staatsministerium der Justiz, dem Staatsministerium für Unterricht und Kultus, dem Staatsministerium für Wissenschaft und Kunst, dem Staatsministerium der Finanzen und für Heimat, dem Staatsministerium für Ernährung, Landwirtschaft, Forsten und Tourismus, dem Staatsministerium für Familie, Arbeit und Soziales, dem Staatsministerium für Gesundheit, Pflege und Prävention und dem Staatsministerium für Digitales wie folgt:

zu 1.a)

Wie viele Straftaten mit Bezug zu Künstlicher Intelligenz wurden in Bayern in den Jahren 2020, 2021, 2022, 2023 und 2024 polizeilich erfasst (bitte tabellarisch nach Jahr, Deliktart, Landkreis/kreisfreier Stadt und Aufklärungsquote angeben)?

zu 2.a)

Wie viele Fälle von Deepfake-Pornografie, manipulierten Audio- oder Videoaufnahmen oder KI-gestützter Identitätsfälschung wurden in Bayern seit 2020 polizeilich bekannt (bitte tabellarisch nach Jahr, Deliktart und Verfahrensstatus angeben)?

zu 3.a)

Wie viele Fälle von Betrug mittels KI-imitierten Stimmen, gefälschten Identitäten oder automatisierten Betrugssystemen wurden in Bayern seit 2020 bekannt (bitte tabellarisch nach Jahr, Schadenshöhe und Verfahrensstatus angeben)?

zu 3.b)

Welche durchschnittliche Schadenshöhe entstand bei diesen Fällen jeweils pro Jahr?

Die Fragen 1.a), 2.a), 3.a) und 3.b) werden aufgrund Sachzusammenhangs gemeinsam beantwortet.

Mangels expliziter, valider Rechercheparameter, die eine automatisierte Auswertung im Sinne der Fragestellungen zulassen, können seitens der Bayerischen Polizei die angefragten Daten auf Basis der Polizeilichen Kriminalstatistik (PKS) nicht erhoben werden.

Stattdessen müssten für die Abfassung eines Antwortbeitrags zu den Fragestellungen 1.a), 2.a), 3.a) und 3.b) umfangreiche manuelle (Einzel-)Auswertungen polizeilicher Akten und Datenbestände erfolgen. Dies würde bei den einzubindenden Polizeidienststellen zu einem erheblichen, in der vorliegenden konkreten Situation nicht vertretbaren zeitlichen und personellen Aufwand führen und die Aufrechterhaltung der effektiven Aufgabenerfüllung der Bayerischen Polizei und damit den ebenfalls verfassungsrechtlich garantierten Schutzauftrag des Staates gegenüber seinen Bürgerinnen und Bürgern gefährden.

Auch unter Berücksichtigung der Bedeutung des sich aus Art. 13 Abs. 2, 16a Abs. 1 und 2 Satz 1 der Verfassung des Freistaates Bayern (BV) ergebenden parlamentarischen Fragerechts der Abgeordneten des Bayerischen Landtags kann daher eine Auswertung von Einzelakten u. Ä. nicht erfolgen.

zu 1.b):

Welche spezifischen Deliktskategorien für KI-bezogene Straftaten hat die Bayerische Polizei in ihrer Kriminalstatistik etabliert oder plant sie zu etablieren?

zu 1.c)

Auf welcher Rechtsgrundlage werden Straftaten als KI-bezogen klassifiziert und statistisch erfasst (bitte auch Methodik angeben)?

Die Fragen 1.b) und 1.c) werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der KI-Bezug bei Straftaten ergibt sich durch die Verwendung von KI-basierten Computerprogrammen als Tatmittel bei der Tatbegehung. Das dabei mögliche Deliktsspektrum ist äußerst vielfältig und reicht u. a. von Urheberrechtsdelikten über Beleidigungs-, Fälschungs- und Vermögensdelikten bis hin zu Erpressungen und Sexualdelikten. Tatmittel werden im Vorgangsbearbeitungssystem der Polizei erfasst, nicht jedoch in der PKS. Die Erfassung eines KI-Bezuges in der PKS über den Deliktsschlüssel ist aufgrund des möglichen umfangreichen Deliktsspektrums nicht zielführend.

In der PKS ist es zwar möglich, spezielle Begehungsweisen, die von kriminalstatistischer Bedeutung bzw. von bedeutendem Auswerteinteresse sind, über das sogenannte PKS-Phänomen zu erfassen. Entsprechende PKS-Phänomenwerte mit KI-Bezug (z. B. Deepfakes) sind aktuell allerdings in der PKS nicht vorhanden.

zu 2.b):

Wie viele dieser Verfahren führten zu Anklagen oder rechtskräftigen Verurteilungen (bitte nach Jahr und verhängten Strafen aufgeschlüsselt angeben)?

Die bayerische Strafverfolgungsstatistik trifft Aussagen zu den Zahlen der Abgeurteilten und Verurteilten. Sie trifft keine Aussagen zu den Hintergründen von Tat, Tätern oder Tatopfern bzw. zu den Modalitäten der Tat. Es wird auch keine Aussage darüber getroffen, ob eine Straftat durch den Einsatz von KI begangen wurde. Das gilt auch für die Justizgeschäftsstatistiken.

Weitere Statistiken, die über den gewünschten Sachverhalt Auskunft geben könnten, gibt es im Geschäftsbereich des Bayerischen Staatsministeriums der Justiz nicht.

Mangels statistischer Daten können die Fragen in der zur Verfügung stehenden Zeit mit vertretbarem Aufwand nicht beantwortet werden. Die Fragen könnten nur beantwortet werden, wenn die Verfahrensakten händisch durchgesehen würden. Dies würde ganz erhebliche Arbeitskraft binden und eine – verfassungsrechtlich gebotene – effektive Strafverfolgung durch die Staatsanwaltschaft gefährden.

zu 2.c):

Welche technischen Kapazitäten zur forensischen Erkennung von Deepfakes und KI-manipulierten Inhalten stehen den bayerischen Strafverfolgungsbehörden zur Verfügung?

Nach Kenntnisstand der Bayerischen Polizei existiert derzeit kein Tool, welches eine valide Deepfake-Erkennung längerfristig durchführen kann, da die technischen Möglichkeiten sich fast täglich weiterentwickeln. Im Rahmen einer Studie der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITIS) hat Versuchen zufolge die manuelle Erkennung durch Fachleute eine höhere Trefferquote als aktuell zur Verfügung stehende Tools. Auch beim Bayerischen Landeskriminalamt (BLKA) stehen keine technischen Kapazitäten zur forensischen Erkennung von Deepfakes und KI-manipulierten Inhalten zur Verfügung. Seitens Justiz und Polizei wird jedoch regelmäßig beobachtet, ob und welche Kapazitäten dieser Art auf dem Markt vorhanden sind und durch die fortschreitende Entwicklung der Kriminalitätsbilder erforderlich werden können.

zu 3.c):

Welche präventiven Maßnahmen hat die Staatsregierung ergriffen, um bayerische Unternehmen und Bürgerinnen und Bürger vor KI-gestütztem Betrug zu schützen?

Es wurden bislang keine eigenständigen Präventionsmaßnahmen bzw. Informationsangebote initiiert, die sich ausschließlich auf die Risiken und Erkennungsmerkmale von KI-gestütztem Betrug beziehen.

Im Rahmen bestehender Präventionsveranstaltungen für Unternehmen (z. B. der Zentralen Ansprechstelle Cybercrime des BLKA – ZAC) wird jedoch regelmäßig darauf hingewiesen, dass verschiedene Straftaten zunehmend auch unter Einsatz von KI-Technologien begangen werden können. Diese Hinweise erfolgen in Vorträgen, Workshops, Online-Formaten sowie in der Öffentlichkeitsarbeit der kriminalpolizeilichen Beratungsstellen. Gleiches gilt für Informationsangebote für Bürgerinnen und Bürger, beispielsweise im Rahmen der polizeilichen Kriminalprävention.

zu 4.a):

Wie viele Beschwerden oder Meldungen über diskriminierende Behandlung durch algorithmische Entscheidungssysteme oder KI-Anwendungen gingen bei bayerischen Behörden seit 2020 ein (bitte tabellarisch nach Jahr, Bereich wie Bewerbung/Kredit/Behördenentscheidung und zuständiger Beschwerdestelle angeben)?

zu 4.b):

Welche dieser Beschwerden führten zu behördlichen Untersuchungen oder Sanktionen (bitte nach Jahr und Ergebnis aufgeschlüsselt angeben)?

zu 4.c):

Welche Anlaufstelle ist in Bayern für Diskriminierungsbeschwerden im Zusammenhang mit KI-Systemen zuständig?

Die Fragen 4.a) – 4.c) werden aufgrund des Sachzusammenhanges gemeinsam beantwortet.

Der Staatsregierung sind keine Beschwerden oder Meldungen über diskriminierende Behandlung durch algorithmische Entscheidungssysteme oder KI-Anwendungen bekannt.

Eine solche Diskriminierung ist auch grundsätzlich nur aufgrund Fehlinterpretationen vorhandener personenbezogener Daten durch ein KI-System denkbar. Innerhalb der Staatsregierung bzw. der Staatsministerien werden Entscheidungen allerdings stets durch deren Beschäftigte getroffen. KI-Systeme dienen hier lediglich der Unterstützung. Eine Diskriminierung aufgrund der Verwendung eines KI-Systems ist daher ausgeschlossen.

zu 5.a):

Wie viele Datenschutzverstöße im Zusammenhang mit KI-Systemen wurden dem Bayerischen Landesbeauftragten für den Datenschutz bzw, den für Datenschutz zuständigen Behörden und Einrichtungen seit 2020 gemeldet (bitte tabellarisch nach Jahr, Art des Verstoßes und verhängten Bußgeldern angeben)?

zu 5.b):

Welche dieser Verstöße betrafen die unbefugte Nutzung personenbezogener Daten zum Training von KI-Modellen?

zu 5.c):

Welche Bußgelder wurden seit 2020 wegen KI-bezogener Datenschutzverstöße verhängt (bitte auch Gesamthöhe der Bußgelder angeben und nach Jahr und betroffenen Unternehmen oder Institutionen aufgeschlüsselt angeben)?

Die Fragen 5.a) bis 5.c) werden aufgrund Sachzusammenhangs gemeinsam beantwortet.

Eine behördenübergreifende Statistik zu Datenschutzverstößen mit und ohne KI-Bezug wird nicht geführt. Art. 33 DSGVO (ggf. in Verbindung mit Art. 28 Abs. 2 S. 2 BayDSG) verpflichtet jeden datenschutzrechtlich Verantwortlichen Datenschutzverstöße an die zuständige Aufsichtsbehörde zu melden.

Meldungen von Verletzungen des Schutzes personenbezogener Daten für den Bereich der öffentlichen Stellen sind in Bayern an den Bayerischen Landesbeauftragten für den Datenschutz (LfD) zu richten. Für Meldungen im nicht-öffentlichen Bereich ist das Landesamt für Datenschutzaufsicht (LDA) zuständig. Für Meldungen von Verletzungen des Schutzes personenbezogener Daten durch Finanzbehörden im Anwendungsbereich der Abgabenordnung ist nach § 32 h Abs. 1 AO die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig.

Die Aufsichtsbehörden sind nicht Teil der Staatsregierung und bei der Erfüllung ihrer Aufgaben gem. Art. 52 Abs.1 DSGVO (ggf. in Verbindung mit Art. 28 Abs. 2 S.1 Nr. 4 BayDSG) völlig unabhängig. Sie unterliegen insbesondere nicht der Kontrolle durch die Staatsregierung. Entsprechend hat der LfD eine Beantwortung der Fragen abgelehnt.

Das LDA teilte mit, dass Datenschutzverstöße im Sinne des Fragenkomplexes 5 nicht bekannt seien.

Die BfDI unterliegt nicht der parlamentarischen Kontrolle durch den Bayerischen Landtag, sondern durch den Deutschen Bundestag.

zu 6.a):

Welche spezialisierten Ermittlungseinheiten oder Schwerpunktstaatsanwaltschaften für KI-bezogene Kriminalität existieren in Bayern?

zu 6.b):

Wie viele Polizeibeamte und Staatsanwälte in Bayern sind speziell für die Verfolgung KI-bezogener Straftaten ausgebildet oder geschult worden (bitte nach Jahr seit 2020 und Schulungsinhalt aufgeschlüsselt angeben)?

zu 6.c):

Welche technischen und personellen Ressourcen sind für die Bekämpfung KI-bezogener Kriminalität derzeit und in Zukunft vorgesehen?

Die Fragen 6.a) bis 6.c) werden aufgrund des Sachzusammenhangs gemeinsam beantwortet. Es wird darauf hingewiesen, dass unter „KI-bezogener Kriminalität“ neben den klassischen Cyberdelikten auch sonstige Straftaten verstanden werden, bei denen KI zum Einsatz kommt. Dabei muss es sich nicht zwingend um Cybercrime-Delikte handeln.

Bayerische Polizei

Derzeit existieren keine spezialisierten Ermittlungseinheiten bei der Bayerischen Polizei, die ausschließlich für die Bearbeitung KI-bezogener Kriminalität zuständig sind. Auch bestehen keine speziellen Ausbildungen oder Lehrgänge, die sich ausschließlich mit KI-bezogener Kriminalität befassen. Allerdings ist diese Bestandteil eigenständiger Cybercrime-Lehrgänge, die für spezialisierte Sachbearbeiter und Sachbearbeiterinnen für diesen Phänomenbereich angeboten werden.

Bei der Bayerischen Polizei wurden flächendeckend „Cybercrime“-Kommissariate bei grundsätzlich jeder Kriminalpolizeiinspektion eingerichtet. Beim BLKA besteht

darüber hinaus das Fachdezernat Cybercrime (Dez. 54) welches zur Erfüllung seiner Aufgaben mit dafür notwendiger Hard- und Software ausgestattet ist. In den Ballungsräumen bestehen zudem mit dem Kriminalfachdezernat 12 in München (seit 1. April 2014) und mit dem Kriminalfachdezernat 5 in Nürnberg (seit 1. Juni 2021) eigens eingerichtete Schwerpunktdienststellen zur kriminalpolizeilichen Bekämpfung von Cybercrime. Die Ausstattung der Dienststellen mit technischen Ressourcen und Personal wird regelmäßig geprüft und dem Stand der Technik entsprechend angepasst.

Aktuell werden über 400 Spezialisten in diesem Bereich eingesetzt. Dabei handelt es sich um ca. 300 speziell aus- und fortgebildete Ermittler bei den Kommissariaten und Dezernaten für Cybercrime und ca. 100 IT-Forensiker, die durch Sicherung und Aufbereitung der digitalen Spuren die Ermittlungen unterstützen.

Daneben wurde die Sonderlaufbahn der IT-Kriminalisten geschaffen. Hierbei werden Informatiker mit entsprechendem Studienabschluss in einer einjährigen polizeifachlichen Unterweisung zu Polizeivollzugsbeamten ausgebildet und unterstützen die Dienststellen in der Bekämpfung der Cyberkriminalität. Mittlerweile werden ca. 200 IT-Kriminalisten bei der Bayerischen Polizei eingesetzt.

Staatsanwaltschaften:

Die im Jahr 2015 gegründete Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg ermittelt bayernweit in besonders herausgehobenen Fällen von Cybercrime. Mit 30 juristisch, technisch und ermittlungstaktisch geschulten Spezialstaatsanwältinnen und -staatsanwälten sowie 4 IT-Forensikern ist die ZCB eine der größten und erfahrensten Spezialstaatsanwaltschaften in Deutschland. Zusätzlich gibt es bei den bayerischen Staatsanwaltschaften jeweils IT-Sonderdezernate und IT-Ansprechpartner, um eine flächendeckende effektive Strafverfolgung im Bereich Cybercrime zu ermöglichen. Sie werden von der ZCB geschult und unterstützt.

Die ZCB verfügt über spezielle Ermittlungseinheiten insbesondere zur Bekämpfung von Kinderpornografie (seit 2020 Zentrum zur Bekämpfung von Kinderpornografie und sexuellem Missbrauch im Internet, ZKI), Cybertrading, Fake Shops, Phishing und Cyberangriffen auf Unternehmen und Einrichtungen (seit 2022 Taskforce „Cyberangriffe auf Unternehmen und Einrichtungen“).

Die ZCB arbeitet eng mit Wissenschaft und Unternehmen zusammen, um moderne innovative Ermittlungswerkzeuge fortzuentwickeln und an die Bedürfnisse der Strafverfolgung anzupassen. Beispiele solcher Kooperationen sind:

- Dark Web Monitor: Webcrawler, der das Internet automatisch durchsucht und dabei verborgene Webseiten im Darknet analysiert und indexiert.
- GraphSense: Blockchain-Analysetool zur Nachverfolgung von Krypto-Zahlungsströmen;
- BigPhish: Tool, um frühzeitig neu-registrierte Domains, die zur Durchführung von auf den Bankensektor bezogenen Phishing-Kampagnen eingerichtet werden, zu detektieren.

Zur Frage der Schulung von Staatsanwälten zu KI-bezogenen Straftaten liegen keine statistisch auswertbaren Daten vor. Das liegt daran, dass auch Fortbildungen, in deren Themenbezeichnung es nicht um KI geht, dennoch KI-bezogene Kriminalität (vgl. oben) inhaltlich behandeln können. Hierzu liegen keine automatisiert auswertbaren Daten der Fortbildungsprogramme und Teilnehmer in den Jahren 2020 bis heute vor.

zu 7.a):

Welche Aufklärungskampagnen oder Informationsangebote hat die Staatsregierung seit 2020 initiiert, um Bürgerinnen und Bürger sowie Unternehmen über Risiken und Erkennungsmerkmale von KI-Missbrauch aufzuklären (bitte tabellarisch nach Jahr, Kampagne, Zielgruppe und Budget angeben)?

Es wurden bislang keine eigenständigen Aufklärungskampagnen bzw. Informationsangebote initiiert, die sich ausschließlich auf die Risiken und Erkennungsmerkmale von KI-Missbrauch beziehen.

Im Rahmen bestehender Präventionskampagnen, z. B. zu den Themen Medienkompetenz, Cybercrime und Betrugsprävention, wird jedoch regelmäßig darauf hingewiesen, dass verschiedene Straftaten zunehmend auch unter Einsatz von KI-Technologien begangen werden können. Diese Hinweise erfolgen in Vorträgen, Workshops, Online-Formaten sowie in der Öffentlichkeitsarbeit der kriminalpolizeilichen Beratungsstellen.

Darüber hinaus wurden in den verschiedenen Ressorts folgende Aufklärungskampagnen bzw. Informationsangebote zur Verfügung gestellt:

Staatsministeriums für Digitales (StMD)

Jahr	Kampagne	Zielgruppe	Budget
2024 fort-laufend	Allianz gegen Desinformation	Techunternehmen, Zivilgesellschaft und Kommunalpolitiker	410.000,00 € in 2025
2024 fort-laufend (GoLive 2025)	Mit Sicherheit Digital	Zivilgesellschaft, Schwerpunkt barrierefreies Angebot	42.000,00 €

Staatsministerium der Finanzen und für Heimat (StMFH)

Im Geschäftsbereich des StMFH fanden darüber hinaus folgende Informationsveranstaltungen statt:

Im Rahmen der Thementage „Kommunale IT-Sicherheit“, die in acht Terminen in jedem Regierungsbezirk durchgeführt wurden, wurden kommunale Vertreter aus ganz Bayern unter anderem auch zu den Gefahren von KI sensibilisiert. Darüber hinaus steht das Landesamt für Sicherheit in der Informationstechnik (LSI) den Kommunen auch zu Gefahren von KI beratend zur Seite.

Betreiber kritischer Infrastrukturen (Kliniken, Trinkwasserversorger und Abwasserentsorger) werden im Rahmen von Vorträgen im Kontext der IT-Sicherheit auch zum Missbrauch von KI sensibilisiert. Bereits existierende Beratungsunterlagen werden schrittweise ergänzt.

Um die digitalen Kompetenzen der Bürger weiter zu stärken, arbeitet das LSI eng mit den BayernLabs zusammen, um zusätzliche Angebote für den sicheren Umgang mit IT zu entwickeln, zum Beispiel in Form einer gemeinsamen Roadshow.

zu 7.b):

Welche Schulungsangebote für Lehrkräfte, Behörden- und Verwaltungsmitarbeitende oder kommunale Entscheidungsträger zum Erkennen und Umgang mit KI-Missbrauch hat die Staatsregierung seit 2020 entwickelt oder gefördert?

Im Rahmen bestehender Fortbildungs- und Präventionsveranstaltungen, insbesondere in den Bereichen Cybercrime, Medienkompetenz und Betrugsprävention, werden auch Aspekte der Nutzung und des möglichen Missbrauchs von KI-Anwendungen thematisiert.

Hierbei ist anzumerken, dass das Thema KI und Kriminalität innerhalb der Präventionsarbeit zunehmend an Bedeutung gewinnt. Entsprechende Konzepte werden derzeit geprüft und bedarfsentsprechend entwickelt.

Ein verantwortungsbewusster und rechtssicherer KI-Einsatz erfordert eine ausreichende Weiterbildung und Qualifizierung des Personals. Für Behörden- und Verwaltungsmitarbeitende gibt es ein breites Angebot, um die erforderlichen Fähigkeiten im Umgang mit KI-Anwendungen sicherzustellen. Zentral werden für Behörden und Beschäftigte Leitfäden zum KI-Einsatz sowie ein E-Learning-Kurs „Künstliche Intelligenz“ bereitgestellt, die im Rahmen der vom StMFH geleiteten ressortübergreifenden KI-Arbeitsgruppe entstanden sind. Der Kurs ist allen staatlichen und kommunalen Beschäftigten auf den Plattformen „BayLern“ und „Digital.Campus Bayern“ zugänglich. Die KI-Leitfäden und der E-Learning-Kurs stellen Maßnahmen zur Vermittlung von KI-Kompetenz im Sinne des Art. 4 der europäischen KI-Verordnung (AI Act) dar. Einzelheiten sind der [Webseite des StMFH](#) zu entnehmen.

Spezifische Schulungsformate, die sich ausschließlich mit der Erkennung oder dem Umgang mit KI-Missbrauch befassen, wurden bislang seitens der Staatsregierung nicht entwickelt.

Zur Sensibilisierung der Beschäftigten in Fragen der IT-Sicherheit stellt das Landesamt für Sicherheit in der Informationstechnik auf BayLern ein ebenfalls zentrales Kursangebot zur Verfügung, das unter anderem das Thema „Sichere Nutzung von Künstlicher Intelligenz (KI)“ behandelt.

Darüber hinaus haben die Ressorts nachfolgende Maßnahmen ergriffen:

Staatsministerium für Familie, Arbeit und Soziales (StMAS)

Das Staatsministerium bietet seinen Mitarbeiterinnen und Mitarbeitern und dem nachgeordneten Geschäftsbereich zusätzlich als Schulung den Hybrid-Vortrag „KI trifft Bürokratie: Innovation oder Illusion?“ im Februar 2026 an. Für die Mitarbeiterinnen und Mitarbeiter des StMAS wurde zudem ein Leitfaden für den Einsatz von KI im Infonet zur Verfügung gestellt.

Staatsministerium für Ernährung, Landwirtschaft, Forsten und Tourismus (StMELF)

Das Staatsministerium für Ernährung, Landwirtschaft, Forsten und Tourismus (StMELF) nutzt zur Schulung der Mitarbeiter im Bereich Künstliche Intelligenz den o.g. E-Learning-Kurs. Mit Ministerialschreiben vom 12. März 2025 sind alle Beschäftigten gebeten, diesen Kurs zu absolvieren. Verpflichtend gilt dies für alle Beschäftigten, die die BayernKI oder andere im Geschäftsbereich freigegebene KI-Werkzeuge nutzen.

Staatsministerium der Finanzen und für Heimat (StMFH)

Um den Herausforderungen durch KI systematisch zu begegnen, wurde seitens des Landesamts für Sicherheit in der Informationstechnik (LSI) am 16. Januar 2025 das Forschungsprojekt „HeCKI – Herausforderungen für die Cybersicherheit durch KI“ offiziell gestartet. Träger dieses Projekts sind das LSI und die Ostbayerische Technische Hochschule (OTH) Amberg-Weiden, die in enger Kooperation an der Schnittstelle zwischen wissenschaftlicher Forschung und praxisnaher Anwendung agieren. Das auf zwei Jahre angelegte Projekt verfolgt das Ziel, die sicherheitsrelevanten Implikationen von KI umfassend zu sammeln, zu analysieren und geeignete Schutzmaßnahmen daraus abzuleiten. Zudem sollen Beratungs- und Schulungsmaterialien für die Zielgruppen des LSI erarbeitet werden.

Staatsministerium für Wohnen, Bau und Verkehr (StMB)

Dem Risiko von KI-Missbrauch innerhalb und gegenüber der Verwaltung wird im Geschäftsbereich des StMB durch den gezielten Aufbau von KI-Kompetenz gemäß Art. 4 der EU-KI-Verordnung und klare, transparente Rahmenbedingungen entgegengewirkt:

- Ergänzend zu den o.g. zentralen Angeboten gibt es spezifische Nutzungshinweise für dienstlich freigegebene KI-Systeme. Entsprechende Freigaben und die Nutzung von KI-Systemen im Allgemeinen sind transparent in einer Dienstvereinbarung geregelt.
- Die Dienstvereinbarung legt für den Geschäftsbereich des StMB zur Prävention von KI-Missbrauch außerdem fest, dass die Eingabe und Verarbeitung personenbezogener oder anderweitig schutzwürdiger Daten in KI-Systeme grundsätzlich nicht erlaubt sind.
- Darüber hinaus haben sich die Einrichtung eines zentralen Intranet-Angebots zum Themenkomplex KI und die klare Benennung von Rahmenbedingungen und Ansprechpartnern für den Einsatz von KI in der Praxis bewährt.
- Die Beschäftigten werden außerdem regelmäßig zu Datenschutz, Informationssicherheit und spezifischen Angriffsmethoden geschult, was auch die Resilienz der Mitarbeitenden gegenüber KI-Missbrauch durch Dritte erhöht. Beispielsweise liegt etwa im Kontext von Phishing-Angriffen ein Fokus auf der Erkennung täuschend echt wirkender Inhalte; wie sie beispielsweise mit KI generiert werden (Deepfakes).

Staatsministerium für Unterricht und Kultus (StMUK)

Lehrkräfte werden u. a. vom KI-Kompetenzzentrum der ALP Dillingen fortgebildet, u. a. mit KI-Selbstlernkurs für Lehrkräfte. Ergänzend werden regionale und schulinterne Fortbildungen angeboten.

Staatsministerium für Wissenschaft und Kunst (StMWK)

Das StMWK hat alle Mitarbeiterinnen und Mitarbeiter sowie die Führungskräfte verpflichtet, den E-Learning-Kurs „Künstliche Intelligenz“ zu absolvieren.

Daneben fand in Zusammenarbeit mit dem Staatsministerium für Digitales und der byte im StMWK am 20. Juni 2024 die „KI-Roadshow“ statt. Ziel war es, einen niederschweligen Zugang zu KI zu ermöglichen und ein grundsätzliches Verständnis für diese Technologie zu schaffen.

In den Jahren 2024 und 2025 hat das StMWK eine Vortragsreihe zum Thema KI in der Verwaltung durch die Leiterin des Staatsinstituts für Hochschulforschung und

Hochschulplanung, Frau Prof. Dr. Welpke (TUM), angeboten. Das StMWK hat darüber hinaus eine interne Arbeitsgruppe zum Einsatz von KI in der Verwaltung mit Mitarbeiterinnen und Mitarbeitern aus allen Abteilungen eingerichtet. Zudem besteht ein enger Erfahrungs- und Informationsaustausch zwischen StMWK, StMFH und dem Digitalverbund der bayerischen Hochschulen. Aus diesem Austausch heraus ist beispielsweise die gemeinsame Informationsveranstaltung am 09.10.2025 von StMFH, StMJ und StMWK zur Europäischen Verordnung über künstliche Intelligenz (KI-VO) konzipiert worden, die sich an alle Beschäftigten in Verwaltung und Justiz gerichtet hat.

Im Intranet des StMWK steht den Beschäftigten ein umfangreiches Informationsangebot zum Einsatz von KI, insbesondere KI-Leitfäden, einschlägige Fortbildungsangebote und rechtliche Grundlagen zur Verfügung.

Staatsministerium des Innern, für Sport und Integration (StMI)

Zusätzlich zu den zentralen Angeboten gibt es spezifische, auf das StMI abgestimmte Nutzungshinweise für den dienstlichen Einsatz von KI-Systemen. Es wurde u.a. eine Intranetseite zum Thema KI im StMI eingerichtet. Diese wird regelmäßig überprüft sowie aktualisiert. Gleiches gilt für die Bayerische Polizei. Für das StMI und den gesamten Geschäftsbereich werden KI-Webinare angeboten, die über Chancen, Gefahren und Risiken von KI informieren und sensibilisieren. Einmal jährlich findet im StMI zudem eine Inhouse-Schulung zum Thema „KI im Arbeitsalltag“ statt, bei der Mitarbeitende umfassend informiert und sensibilisiert werden.

zu 7.c):

Wie bewertet die Staatsregierung die Wirksamkeit dieser Präventionsmaßnahmen anhand messbarer Indikatoren?

Da bislang keine spezifischen Präventionsmaßnahmen ausschließlich zum Thema KI-Missbrauch durchgeführt wurden, ist uns eine Aussage bezüglich der Wirksamkeit solcher Maßnahmen nicht möglich.

zu 8.a):

Welche Kooperationen hat die Staatsregierung seit 2020 mit anderen Bundesländern, Bundesbehörden oder internationalen Partnern zur Bekämpfung KI-bezogener Kriminalität etabliert (bitte tabellarisch nach Jahr, Partner, Thema und Ergebnis angeben)?

Derzeit bestehen keine Kooperationen der Staatsregierung mit anderen Bundesländern, Bundesbehörden oder internationalen Partnern, die sich ausschließlich mit der Bekämpfung KI-bezogener Kriminalität befassen. Unbenommen hiervon kooperiert die Staatsregierung, insbesondere im Rahmen polizeilicher und justizieller Zusammenarbeit mit anderen Ländern und Staaten bei der Bekämpfung von Cyberkriminalität (z. B. über EUROPOL, INTERPOL). KI-bezogene Straftaten spielen hierbei eine zunehmend bedeutsame Rolle.

Seitens des StMJ fand dabei insbesondere folgende Kooperation statt, wobei sich diese nicht ausschließlich auf die Bekämpfung KI-bezogener Straftaten bezieht:

Jahr	Partner	Thema	Ergebnis
2024	Interpol	Kontinuierliche Zusammenarbeit bei der Bekämpfung von Cybercrime zwischen ZCB und Interpol (v. a. Schutz von Kindern vor sexueller Ausbeutung; grenzüberschreitende Cybercrime in der Wirtschafts- und Finanzwelt)	Regelmäßige gemeinsame Durchführung des New Technologies Expert Forum, Beteiligung am 41. Operational Meeting der Specialist Group on Crimes against Children, Einbindung in das Projekt RESCUE zur Bekämpfung des aus Südostasien heraus begangenen Cyberbetrugs

zu 8.b):

Welche Best-Practice-Beispiele aus anderen Bundesländern oder Staaten zur Erfassung, Verfolgung und Prävention KI-bezogener Straftaten sind der Staatsregierung bekannt und wurden in Bayern übernommen?

Derzeit sind hier keine übernahmefähigen und hinreichend validierten Best-Practice-Beispiele aus anderen Bundesländern oder Staaten bekannt.

zu 8.c):

Welche gesetzgeberischen Initiativen plant die Staatsregierung auf Bundes- oder Landesebene, um Strafbarkeitslücken bei KI-Missbrauch zu schließen?

Die Staatsregierung beobachtet und prüft die Entwicklungen der Kriminalität fortwährend auf gesetzgeberischen Handlungsbedarf. Dies gilt auch für Taten, die unter Einsatz von Künstlicher Intelligenz begangen werden. Zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes hat die Staatsregierung bereits 2024 einen Gesetzentwurf in den Bundesrat eingebracht (BR-Drs. 222/24) und diesen, nachdem er der Diskontinuität anheimgefallen war, im Juni dieses Jahres erneut in den Bundesrat eingebracht (BR-Drs. 272/25). Weitere gesetzgeberische Initiativen zum (Bundes-)Strafrecht sind derzeit nicht geplant.

Mit freundlichen Grüßen

gez. Sandro Kirchner
Staatssekretär