Zwischen Bedrohung und Chance: Der Einfluss von KI auf die Cybersicherheit

it-sa, Nürnberg, Knowledge Forum A, 23.10.2024

RA und FA-IT-Recht Steffen Batscheider

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

Steffen Batscheider

Rechtsanwalt & Fachanwalt für IT-Recht

in Nürnberg

www.kanzlei-batscheider.de

info@kanzlei-batscheider.de

rechtsanwalt SB

Rechtsanwaltskanzlei Batscheider

KI IN IT-SICHERHEIT:

ANWENDUNG

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI IN IT-SICHERHEIT: ANWENDUNG

- **Bedrohungserkennung**
  - Analyse großer Datenmengen zur Identifizierung verdächtiger Aktivitäten
- **Automatisierte Reaktionen**
  - KI ermöglicht schnellere und effizientere Reaktionen auf Sicherheitsvorfälle
- **Vorhersage**
  - KI kann potentielle zukünftige Bedrohungen vorhersagen
- **Identität**
  - KI wird zur Identitätsprüfung eingesetzt, die Authentifizierung wird verbessert
- **Anomalien**
  - Anomalien können durch KI-Systeme erkannt werden

KI IN IT-SICHERHEIT: ANWENDUNG

- RECHTLICHE IMPLIKATINEN -

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

www.kanzlei-batscheider.de

KI IN IT-SICHERHEIT: ANWENDUNG - RECHTLICHE IMPLIKATIONEN -

Bei Hochrisiko-KI-Systemen (Art. 6 KI-VO, insbesondere Anhang III KI-VO) **wie**

- KRITIS
- Bildungsbereich zur Überwachung & Erkennung verbotenen Verhaltens
- Kreditwürdigkeitsprüfung & Bonitätsbewertung natürlicher Personen

➢ **Folge:**

- Konformitätsbewertung (Art. 43 KI-VO)
- Einhaltung Anforderungen an Datenqualität, Transparenz, menschliche Aufsicht (Art. 14 KI-VO)

§ 30 BSIG

- (Besonders) wichtige Einrichtungen müssen angemessene und verhältnismäßige TOMs treffen (Stand der Technik)

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI IN IT-SICHERHEIT: ANWENDUNG - RECHTLICHE IMPLIKATIONEN -

Bei Hochrisiko-KI-Systemen (Art. 6 KI-VO, insbesondere Anhang III KI-VO) **wie**

- KRITIS
- Bildungsbereich zur Überwachung & Erkennung verbotenen Verhaltens
- Kreditwürdigkeitsprüfung & Bonitätsbewertung natürlicher Personen

➢ **Folge:**

- Konformitätsbewertung (Art. 43 KI-VO)
- Einhaltung Anforderungen an Datenqualität, Transparenz, menschliche Aufsicht (Art. 14 KI-VO)

§ 30 BSIG

- (Besonders) wichtige Einrichtungen müssen angemessene und verhältnismäßige TOMs treffen (Stand der Technik)

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI IN IT-SICHERHEIT: ANWENDUNG - RECHTLICHE IMPLIKATIONEN -

- Datenschutzrechtliche Aspekte
  - DSGVO durch spezifische Bestimmungen der KI-VO ergänzt
  - BSIG regelt Verarbeitung personenbezogener Daten durch BSI (§§ 20 ff. BSIG)
- KI-VO bildet den Rechtsrahmen
- BSIG
  - Wird KI-VO im Bereich der Netz- & Informationssicherheit ergänzen
  - Wird zusätzliche Anforderungen an Cybersicherheit besonders wichtiger und wichtiger Einrichtungen
- Compliance-Anforderungen
  - Z.B. Risikomanagement, Dokumentation, regelmäßige Audits, TOMs (KI-VO & BSIG)

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI IN IT-SICHERHEIT: ANWENDUNG - RECHTLICHE IMPLIKATIONEN -

- **Datenschutzrechtliche Aspekte**
  - DSGVO durch spezifische Bestimmungen der KI-VO ergänzt
  - BSIG regelt Verarbeitung personenbezogener Daten durch BSI (§§ 20 ff. BSIG)
- KI-VO bildet Rechtsrahmen für KI-Systeme in EU
- BSIG
  - Wird KI-VO im Bereich der Netz- & Informationssicherheit ergänzen
  - Wird zusätzliche Anforderungen an Cybersicherheit besonders wichtiger und wichtiger Einrichtungen
- Compliance-Anforderungen
  - Z.B. Risikomanagement, Dokumentation, regelmäßige Audits, TOMs (KI-VO & BSIG)

KI IN IT-SICHERHEIT: ANWENDUNG - RECHTLICHE IMPLIKATIONEN -

- **Datenschutzrechtliche Aspekte**
  - DSGVO durch spezifische Bestimmungen der KI-VO ergänzt
  - BSIG regelt Verarbeitung personenbezogener Daten durch BSI (§§ 20 ff. BSIG)
- **KI-VO bildet Rechtsrahmen für KI-Systeme in EU**
- **BSIG**
  - Wird KI-VO im Bereich der Netz- & Informationssicherheit ergänzen
  - Wird zusätzliche Anforderungen an Cybersicherheit besonders wichtiger und wichtiger Einrichtungen
- Compliance-Anforderungen
  - Z.B. Risikomanagement, Dokumentation, regelmäßige Audits, TOMs (KI-VO & BSIG)

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI IN IT-SICHERHEIT: ANWENDUNG - RECHTLICHE IMPLIKATIONEN -

- **Datenschutzrechtliche Aspekte**
  - DSGVO durch spezifische Bestimmungen der KI-VO ergänzt
  - BSIG regelt Verarbeitung personenbezogener Daten durch BSI (§§ 20 ff. BSIG)
- **KI-VO bildet Rechtsrahmen für KI-Systeme in EU**
- **BSIG**
  - Wird KI-VO im Bereich der Netz- & Informationssicherheit ergänzen
  - Wird zusätzliche Anforderungen an Cybersicherheit besonders wichtiger und wichtiger Einrichtungen
- **Compliance-Anforderungen**
  - Z.B. Risikomanagement, Dokumentation, regelmäßige Audits, TOMs (KI-VO & BSIG)

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI-GESTÜTZTE ANGRIFFE:

POTENTIAL

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI-GESTEUERTE ANGRIFFE: POTENTIAL

Automatisierte Social Engineering Angriffe

- **Manipulation** einer Person zu Zwecken der Preishabe persönlicher / finanzieller Informationen oder auch Überlassung von Kontrolle über ein Computersystem
  - Z.B. personalisierte Phising-E-Mails durch KI-Systeme
  - Deepfake-Betrug
    - Stimmenimitation & Gesichter in Videos ersetzen anhand verfügbarer Videos und Audiodateien

- Rechtliches
  - Verbot von KI-Systemen, die menschliches Verhalten manipulieren (Art. 5 KI-VO)
  - Betrug & Datenveränderung (§§ 263, 303a StGB)
  - Meldepflicht für Sicherheitsvorfälle (§ 32 BSIG)

KI-GESTEUERTE ANGRIFFE: POTENTIAL

Automatisierte Social Engineering Angriffe

- **Manipulation** einer Person zu Zwecken der Preishabe persönlicher/finanzieller Informationen oder auch Überlassung von Kontrolle über ein Computersystem
  - Z.B. personalisierte Phising-E-Mails durch KI-Systeme
  - Deepfake-Betrug
    - Stimmenimitation & Gesichter in Videos ersetzen anhand verfügbarer Videos und Audiodateien

- **Rechtliches**
  - Verbot von KI-Systemen, die menschliches Verhalten manipulieren (Art. 5 KI-VO)
  - Betrug & Datenveränderung (§§ 263, 303a StGB)
  - Meldepflicht für Sicherheitsvorfälle (§ 32 BSIG)

KI-GESTEUERTE ANGRIFFE: POTENTIAL

KI-generierte Malware

- **Viren, Würmer,** die in Computersysteme eindringen und dort Störungen oder Schäden verursachen
  - Anpassungsfähig & umgehen Abwehrmechanismen
  - Entwickeln sich selbständig weiter
  - (M.W.) derzeit kein bestätigter Fall vollständig autonomer & sich selbst weiterentwickelnder Malware

- Rechtliches
  - Ggf. könnten KI-Systeme zur Generierung von Malware verbotene KI-Praktiken fallen (Art. 5 KI-VO)
  - Vorbereitung einer Straftat (§ 202c StGB)
  - Möglichkeit der Untersuchung von Systemen (§ 14 BSIG)

KI-GESTEUERTE ANGRIFFE: POTENTIAL

KI-generierte Malware

- **Viren, Würmer,** die in Computersysteme eindringen und dort Störungen oder Schäden verursachen
  - Anpassungsfähig & umgehen Abwehrmechanismen
  - Entwickeln sich selbständig weiter
  - (M.W.) derzeit kein bestätigter Fall vollständig autonomer & sich selbst weiterentwickelnder Malware

- **Rechtliches**
  - Ggf. könnten KI-Systeme zur Generierung von Malware verbotene KI-Praktiken fallen (Art. 5 KI-VO)
  - Vorbereitung einer Straftat (§ 202c StGB)
  - Möglichkeit der Untersuchung von Systemen (§ 14 BSIG)

KI-GESTEUERTE ANGRIFFE: POTENTIAL

Angriffe auf KI-Systeme selbst (adversarial attacks)

- **Ziel:** Untergraben der Integrität und Zuverlässigkeit von KI-Systemen
  - Täuschung von KI-Modellen durch manipulierte Eingabedaten
  - Vergiften von Trainingsdaten zu Zwecken der Beeinträchtigung von KI-Systemen
  - Vertrauliche Informationen können aus KI-Modellen extrahiert werden

- Rechtliches
  - KI-VO: ggf. indirekte Relevanz von Regelungen (z.B. *Robustheit gegenüber Fehlern & Inkonsistenz von Hochrisiko-KI-Systemen (Art. 15 KI-VO) und zur verpflichtenden Identifizierung & Analyse von Risiken (Art. 9 KI-VO)*
  - Computersabotage (§ 303b StGB)
  - Möglichkeit der automatisierten Datenauswertung durch BSI zur Erkennung von Schadprogrammen und sonstiger Gefahren einschl. deren Abwehr (§ 8 BSIG)

KI-GESTEUERTE ANGRIFFE: POTENTIAL

Angriffe auf KI-Systeme selbst (adversarial attacks)

- **Ziel:** Untergraben der Integrität und Zuverlässigkeit von KI-Systemen
  - Täuschung von KI-Modellen durch manipulierte Eingabedaten
  - Vergiften von Trainingsdaten zu Zwecken der Beeinträchtigung von KI-Systemen
  - Vertrauliche Informationen können aus KI-Modellen extrahiert werden

- **Rechtliches**
  - KI-VO: ggf. indirekte Relevanz von Regelungen (z.B. *Robustheit gegenüber Fehlern & Inkonsistenz von Hochrisiko-KI-Systemen* (Art. 15 KI-VO) und zur *verpflichtenden Identifizierung & Analyse von Risiken* (Art. 9 KI-VO)
  - Computersabotage (§ 303b StGB)
  - Automatisierte Datenauswertung durch BSI zur Gefahrenerkennung und Abwehr (§ 8 BSIG)

KI-GESTÜTZTE ANGRIFFE:

GEDANKEN ZU HAFTUNG

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI-GESTEUERTE ANGRIFFE: GEDANKEN ZU HAFTUNG

Zivilrechtliche Haftungsfragen werden komplexer

- Vorschlag einer EU-KI-Haftungs-RL (2022/0303(COD)) zur Anpassung der Vorschriften über <u>außervertragliche zivilrechtliche Haftung</u>
  - § 823 BGB dürfte als verschuldensabhängige Schadensersatznorm weiter Anwendung finden
  - Offenlegungspflicht *(Herausgabeverlangen von Informationen zu KI-System, zur Ermittlung potenzieller Ansprüche und Anspruchsgegner sowie zur Untersuchung des KI-Systems auf Fehler oder Sicherheitslücken)*
  - Widerlegliche Kausalvermutung für eingetretenen Schaden aufgrund Verletzung einer Sorgfaltspflicht nach z.B. der KI-VO
- BSIG sieht Bußgeldvorschriften vor (§ 65 BSIG)
- Verantwortlichkeit (Entwickler, Nutzer, KI-System selbst)
- Problem: Zuordnung von Schuld & Verantwortung bei gewissem Grad an Autonomie

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI-GESTEUERTE ANGRIFFE: GEDANKEN ZU HAFTUNG

Zivilrechtliche Haftungsfragen werden komplexer

- Vorschlag einer EU-KI-Haftungs-RL (2022/0303(COD)) zur Anpassung der Vorschriften über <u>außervertragliche zivilrechtliche Haftung</u>
  - § 823 BGB dürfte als verschuldensabhängige Schadensersatznorm weiter Anwendung finden
  - Offenlegungspflicht *(Herausgabeverlangen von Informationen zu KI-System, zur Ermittlung potenzieller Ansprüche und Anspruchsgegner sowie zur Untersuchung des KI-Systems auf Fehler oder Sicherheitslücken)*
  - Widerlegliche Kausalvermutung für eingetretenen Schaden aufgrund Verletzung einer Sorgfaltspflicht nach z.B. der KI-VO
- BSIG sieht Bußgeldvorschriften vor (§ 65 BSIG)
- Verantwortlichkeit (Entwickler, Nutzer, KI-System selbst)
- Problem: Zuordnung von Schuld & Verantwortung bei gewissem Grad an Autonomie

KI-GESTEUERTE ANGRIFFE: GEDANKEN ZU HAFTUNG

Neue Herausforderungen in der Strafverfolgung

- Verstärkte internationale Zusammenarbeit erforderlich

- BSIG sieht BSI als zentrale Meldestelle für Meldungen von Dritten und wertet diese aus (§ 5 BSIG)
    - Ermöglicht zentrale Sammlung von Informationen über KI-gestützte Angriffe & weiterer Cybersicherheitsrisiken

- Mitgliedsstaaten müssen notifizierende & den Markt überwachende Behörden einrichten, ausstatten und kompetentes Personal beschäftigen (Art. 70 KI-VO)
    - Mitarbeiter: Fachwissen & tiefes Verständnis der KI-Technologien, Cybersicherheit, Datenschutz, Grundrechte u.a.

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

KI-GESTEUERTE ANGRIFFE: GEDANKEN ZU HAFTUNG

Neue Herausforderungen in der Strafverfolgung

- Verstärkte internationale Zusammenarbeit erforderlich

- BSIG sieht BSI als zentrale Meldestelle für Meldungen von Dritten und wertet diese aus (§ 5 BSIG)
    - Ermöglicht zentrale Sammlung von Informationen über KI-gestützte Angriffe & weiterer Cybersicherheitsrisiken

- Mitgliedsstaaten müssen notifizierende & den Markt überwachende Behörden einrichten, ausstatten und kompetentes Personal beschäftigen (Art. 70 KI-VO)
    - Mitarbeiter: Fachwissen & tiefes Verständnis der KI-Technologien, Cybersicherheit, Datenschutz, Grundrechte u.a.

KI-GESTEUERTE ANGRIFFE: GEDANKEN ZU HAFTUNG

Neue Herausforderungen in der Strafverfolgung

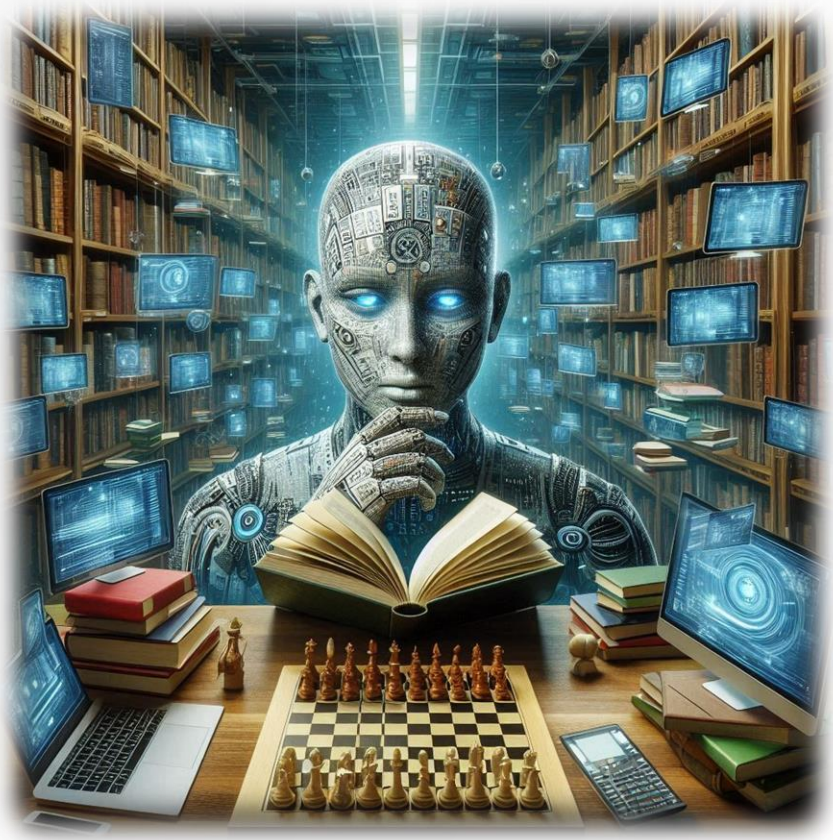
- Verstärkte internationale Zusammenarbeit erforderlich

- BSIG sieht BSI als zentrale Meldestelle für Meldungen von Dritten und wertet diese aus (§ 5 BSIG)
  - Ermöglicht zentrale Sammlung von Informationen über KI-gestützte Angriffe & weiterer Cybersicherheitsrisiken

- Mitgliedsstaaten müssen notifizierende & den Markt überwachende Behörden einrichten, ausstatten und kompetentes Personal beschäftigen (Art. 70 KI-VO)
  - Mitarbeiter: Fachwissen & tiefes Verständnis der KI-Technologien, Cybersicherheit, Datenschutz, Grundrechte u.a.

KI IN DER IT-SICHERHEIT:

ETHIK & STRATEGIE



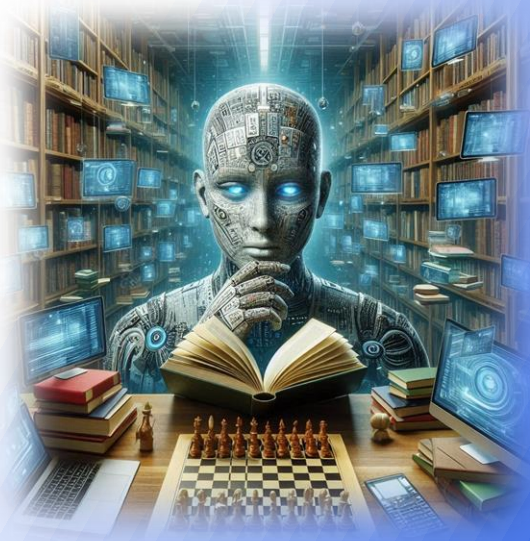
rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

KI IN DER IT-SICHERHEIT: ETHIK & STRATEGIE

Ethik

- Ethische Richtlinien sind unerlässlich
  - KI-VO kodifiziert auch in Cybersicherheit zu beachtende Grundsätze (Art. 4 & Art. 5 KI-VO)
  - KI-VO fordert angemessene menschliche Aufsicht (Art. 14 KI-VO)



Strategisches

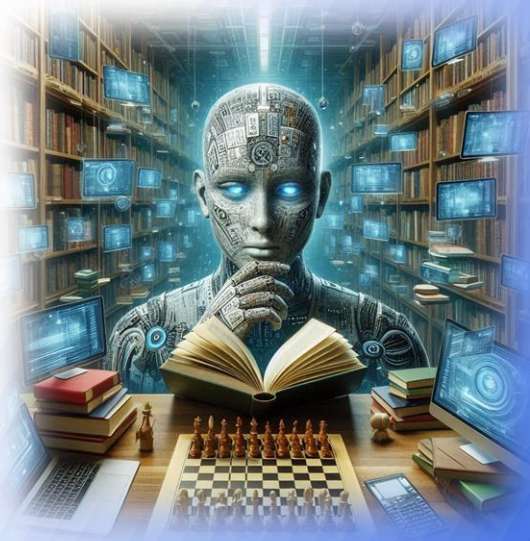
- Internationale Kooperation & Regulierung sind notwendig
  - Cybersicherheitsbedrohungen sind grenzüberschreitender Natur, sodass globale Standards für KI notwendig sind
  - KI-VO fördert dies, indem sie eine staatenübergreifende Zusammenarbeit vorsieht (Art. 70 & Art. 71 KI-VO)

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

KI IN DER IT-SICHERHEIT: ETHIK & STRATEGIE

Ethik

- Ethische Richtlinien sind unerlässlich
  - KI-VO kodifiziert auch in Cybersicherheit zu beachtende Grundsätze (Art. 4 & Art. 5 KI-VO)
  - KI-VO fordert angemessene menschliche Aufsicht (Art. 14 KI-VO)



Strategisches

- Internationale Kooperation & Regulierung sind notwendig
  - Cybersicherheitsbedrohungen sind grenzüberschreitender Natur, sodass globale Standards für KI notwendig sind
  - KI-VO fördert dies, indem sie eine staatenübergreifende Zusammenarbeit vorsieht (Art. 70 & Art. 71 KI-VO)

Steffen Batscheider
Rechtsanwalt & Fachanwalt für IT-Recht

VIELEN DANK!

Steffen Batscheider

Rechtsanwalt
Fachanwalt für IT-Recht

Nürnberg

www.kanzlei-batscheider.de

info@kanzlei-batscheider

Scan me

rechtsanwalt SB
Rechtsanwaltskanzlei Batscheider