



Expert Evidence in Criminal Proceedings Involving AI?

Thomas Hrdinka

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

December 18, 2023

SACHVERSTÄNDIGENBEWEIS IM STRAFVERFAHREN MIT KI?

Thomas Hrdinka

Zivilingenieur, Universität Wien
Ocwirkgasse 22, 1210 Wien, AT
thrdinka@zth.at; <http://www.zth.at>

Schlagworte: *Künstliche Intelligenz, Strafverfahren, Beweismittel, IT-Forensik*

Abstract: *Im Bereich des IT-Strafrechts ist es aufgrund der über die Jahre stetig steigenden Datenmengen gegeben, dass die Aufwände zur Beweissicherung und Analyse der Daten analog dazu – trotz der gestiegenen Rechenleistungen – ansteigt. Der Einsatz entsprechender forensischer Werkzeuge ist daher geboten. Diese Technologien unterstützen Forensiker dabei, Ergebnisse in kurzer Zeit zu erhalten, welche diese bei manueller Sichtung niemals erhalten hätten. Allerdings sollten sich sie nicht von solchen Ergebnissen hinreißen lassen, und voreilige und womöglich falsche Schlussfolgerungen zu tätigen. Dieses als „Bias“ bekannte Phänomen ist die systematische fehlerhafte Neigung beim Wahrnehmen, Erinnern, Denken und Urteilen. Die in jüngster Zeit aufgekomenen KI-Systeme könnten daher eine innovative Methode darstellen, Sachverständige dabei zu unterstützen einerseits rasch zu Ergebnissen zu kommen, und andererseits durch diese „künstliche Intelligenz“ einem Bias zu entgehen, und so die Qualität der Befundaufnahmen und Gutachten zu erhöhen. Diese Arbeit beschäftigt sich mit Möglichkeiten eine KI sinnvoll in der Gutachtensarbeit einzusetzen, und zeigt auch dabei die Grenzen anhand von Beispielen auf. Erforscht wurde anhand von „Google Bard“, dass die Generierung technischer Anforderungen, wie bspw. einem Testprogramm oder einem Datenmodell mit Testdaten nahezu perfekte Ergebnisse liefert, welche der Sachverständigenarbeit zeitsparend zugute kommt. Hingegen kann gezeigt werden, wenn Fragestellungen im interdisziplinären Bereich gestellt werden, wie das Ziehen rechtsrelevanter Schlüsse, KI-Systeme mit falschen Ergebnissen vollkommen versagen.*

1. Einleitung

Gem. § 125 Z. 1 StPO¹ ist „Sachverständiger“ eine Person, die auf Grund besonderen Fachwissens in der Lage ist, beweiserhebliche Tatsachen festzustellen (Befundaufnahme) oder aus diesen rechtsrelevante Schlüsse zu ziehen und sie zu begründen (Gutachtenserstattung). Er ist zu bestellen, wenn für Ermittlungen oder für Beweisaufnahmen besonderes Fachwissen erforderlich ist, über welches die Strafverfolgungsbehörden durch ihre Organe, besondere Einrichtungen oder bei ihnen dauernd angestellte Personen nicht verfügen. Sachverständige haben den Befund und das Gutachten nach bestem Wissen und Gewissen und nach den Regeln ihrer Wissenschaft oder Kunst oder ihres Gewerbes abzugeben (§ 127 Abs. 2). Davon strikt zu unterscheiden ist gem. § 249 Abs. 3 eine „Person mit besonderem Fachwissen“ (vgl. „Privatsachverständiger“), die der Angeklagte zur Befragung eines Sachverständigen beiziehen kann, und dem ein Sitz neben dem Verteidiger zu gestatten ist. Diese darf den Verteidiger bei der Fragestellung unterstützen oder selbst Fragen zu Befund und Gutachten an den Sachverständigen richten. Befund und Gutachten bilden daher einen zentralen Bestandteil im Strafverfahren, aus dem rechtsrelevante Schlüsse gezogen werden, denn für die Bestimmung der Schuld oder Unschuld des Angeklagten muss mit an Sicherheit grenzender Wahrscheinlichkeit feststehen, dass kein Freispruchgrund vorliegt.² Aus diesen Gründen ist es essenziell, dass das Gutachten auf fehlerfrei erhobenen Fakten, den Befundungsgrundlagen, beruht.

¹ Strafprozessordnung, BGBl 631/1975, i.d.g.F.

² Vgl. dazu die freie Beweiswürdigung gem. § 14 StPO und den Freispruch gem. § 259 Abs. 3.

2. Beispielfall

Anhand eines realen Beispielfalls soll die Einsatzfähigkeit von Google Bard getestet werden. Bard ist Googles experimenteller KI-Chat-Dienst, ähnlich wie ChatGPT, welcher seit Mai 2023 auf dem LLM PaLM³ basiert. Der größte Unterschied zu ChatGPT ist, dass Bard mit Informationen aus dem Web arbeitet, was veraltete Informationen oder Unwissen vermeiden soll.

Ausgangspunkt ist ein „Hacking“-Fall, wo für die StA Befund und Gutachten zu erstatten war, ob ein wg. § 118a⁴ StGB⁵ Verdächtiger nachzuweisen ist, bzw. ob noch weitere Ermittlungen nötig sind. Der Vorhalt des Geschädigten, einem Betreiber eines Internetportals für Kontakte, war, dass Daten seiner Kunden gelöscht oder deren Passwörter geändert wurden. Der Tatverdächtige betrieb selbst ein vergleichbares Portal, das als Konkurrenz gelten konnte.

2.1. Technische Untersuchung

Unter Zuhilfenahme der befundeten Dateien, speziell dem Access-Log des Webservers und den Informationen aus der IP-Adressenauswertung gem. Gerichtsakt wurde versucht Spuren zu einem Angriff finden und den Angriff zu rekonstruieren. Diese Arbeit wurde 2014 manuell mit Hilfe selbst programmierter Hilfswerkzeuge gelöst. Es soll nun untersucht werden, ob und wie eine KI am Bsp. Bard unterstützen könnte.

Im ersten Schritt muss das Access-Log-File entweder in die Datenbank importiert werden, oder zeitsparender als external Table der Datenbank zugänglich gemacht werden:

Bard Prompt:

```
Generiere ein Oracle SQL Script für folgendes access.log eines Webservers. Es muss eine External Table definiert werden, um die Daten aus der Datenbank zu analysieren: nn.nnn.nnn.nnn - - [19/Mar/2013:00:00:00 +0100] "GET /images/singlebannerneu8.jpg HTTP/1.1" 200 39410 www.abcdefgh.de "http://www.abcdefgh.de/" "Mozilla/5.0 (Windows NT 5.1; rv:19.0) Gecko/20100101 Firefox/19.0" "-"
```

Ergebnis:

```
-- Erstellen eines neuen Directory-Pfads
CREATE OR REPLACE DIRECTORY access_logs AS '/var/log/apache2';

-- Erstellen der externen Tabelle
CREATE TABLE access_log (
  ip_address VARCHAR2(15),
  user_agent VARCHAR2(255),
  date_time DATE,
  method VARCHAR2(10),
  request VARCHAR2(255),
  status VARCHAR2(10),
  bytes VARCHAR2(255),
  referer VARCHAR2(255),
```

3 CHOWDHERY, NARANG, DEVLIN et al: PaLM: Scaling Language Modeling with Pathways, arXiv:2204.02311v5.

4 Der Fall wurde im Juni 2014 untersucht. Die Fassung des § 118a Abs. 1 StGB „Widerrechtlicher Zugriff auf ein Computersystem“ lautete zu diesem Zeitpunkt: „Wer sich in der Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem überwindet, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“

5 Strafgesetzbuch, BGBl 60/1974 i.d.g.F,

```

referrer_domain VARCHAR2(255)
) ORGANIZATION EXTERNAL (
  TYPE oracle_loader
  DEFAULT DIRECTORY access_logs
  ACCESS PARAMETERS (
    RECORDS DELIMITED BY NEWLINE
    badfile access_logs:'access_log.bad'
    logfile access_logs:'access_log.log'
    fields terminated by ' '
    missing field values are null
    (ip_address, user_agent, date_time, method, request, status, bytes, referer, referrer_domain)
  )
  LOCATION ('access_log')
) REJECT LIMIT UNLIMITED;

```

Das Ergebnis ist nahezu korrekt, und mangelt lediglich an der fehlenden Berücksichtigung der Zeitzone beim Attribut `date_time`. Ebenso ist die genaue Abgrenzung und Aufteilung der Attribute verbesserungswürdig. Es sollen nun anhand dieser Tabelle die Administratorzugänge untersucht werden.

Bard Prompt:

```
Ermittle mit SQL aus access_log alle Requests die Administratoren machten.
```

Ergebnis:

```

SELECT
  ip_address, user_agent, date_time, method, request, status, bytes, referer, referrer_domain
FROM
  access_log
WHERE
  user_agent LIKE '%admin%';

```

Auch dieses Ergebnis ist grds. korrekt, allerdings könnte ein Administrator Zugang auch aus der URL (im Attribut `request`) codiert sein. Da ein SQL Injection Angriff angenommen werden muss, wird schließlich eine komplexere Abfrage gestellt.

Bard Prompt:

```
Ermittle mit SQL aus access_log alle Requests die auf eine SQL Injection hinweisen. Die URL muss vorher unescaped werden.
```

Ergebnis:

```

WITH unescaped_requests AS (
  SELECT
    ip_address, user_agent, date_time, method, UNESCAPE_STRING(request) AS request, status,
    bytes, referer, referrer_domain
  FROM
    access_log
)
SELECT
  ip_address, user_agent, date_time, method, request, status, bytes, referer, referrer_domain
FROM

```

```

unescaped_requests
WHERE
(
  request LIKE '%' || ';' || '%'
OR request LIKE '%' || '\'' || '%'
OR request LIKE '%' || '"' || '%'
OR request LIKE '%' || 'union' || '%'
OR request LIKE '%' || 'select' || '%'
OR request LIKE '%' || 'from' || '%'
OR request LIKE '%' || 'where' || '%'
);

```

Auch dieses Ergebnis ist grds. korrekt, allerdings existiert in Oracle keine Funktion UNESCAPE_STRING. Statt dessen hätte die Oracle Funktion UTL_URL.UNESCAPE verwendet werden müssen. Letztlich wird festgestellt, dass ein Einsatz von Bard zwecks Generierung von Tools geeignet ist, wobei die Ergebnisse noch nachbearbeitet werden müssen.

2.2. Weitere, interdisziplinäre Untersuchungen

In einem ersten Schritt sollen die Rechtsgrundlagen für Österreich ermittelt werden, um zu erfahren, ob und wie die Beweise verarbeitet werden dürfen.

Bard Prompt:

```

Wie kann eine Hackerangriff mittels access_log aufgrund geltender Rechtsgrundlagen in Österreich ermittelt werden? Welche Ermittlungen sind nicht erlaubt?

```

Ergebnis:

Ein Hackerangriff mittels access_log kann in Österreich aufgrund folgender Rechtsgrundlagen ermittelt werden:

- **§ 90 StPO:** Durchsuchungsbeschluss
- **§ 91 StPO:** Beschlagnahme
- **§ 92 StPO:** Auskunftersuchen
- **§ 93 StPO:** Ermittlungsanordnungen

Der **Durchsuchungsbeschluss** kann angeordnet werden, um den access_log oder andere Beweismittel zu beschlagnahmen. Dazu muss ein Richter oder Staatsanwalt einen Durchsuchungsbeschluss erlassen, der die Durchsuchung des Computers oder des Netzwerks, auf dem sich der access_log befindet, anordnet.

Die **Beschlagnahme** kann auch ohne Durchsuchungsbeschluss angeordnet werden, wenn der access_log oder andere Beweismittel in Gefahr sind, verloren zu gehen oder vernichtet zu werden.

Das **Auskunftersuchen** kann angeordnet werden, um den Betreiber des Servers oder des Netzwerks, auf dem sich der access_log befindet, zur Auskunft über den access_log zu verpflichten.

Die **Ermittlungsanordnung** kann angeordnet werden, um die Polizei oder eine andere Ermittlungsbehörde zu ermächtigen, den access_log zu untersuchen.

Ermittlungen, die nicht erlaubt sind, sind:

- **Die Durchsuchung des Computers oder des Netzwerks des Opfers ohne Durchsuchungsbeschluss oder Auskunftersuchen**
- **Der Zugriff auf den access_log ohne Zustimmung des Betreibers des Servers oder des Netzwerks**
- **Die Verwendung von Schadsoftware oder anderer illegaler Methoden zur Erlangung des access_logs**

Die Ermittlungen in einem Hackerangriffsfall sind in Österreich streng reglementiert. Die Polizei oder eine andere Ermittlungsbehörde darf nur dann auf den access_log zugreifen, wenn sie dafür eine rechtliche Grundlage hat.

Semantisch gemeint war bei der Anfrage, wie mittels access_log aufgrund geltender Rechtslage der Hackerangriff untersucht werden darf, was auch in Richtung Ermittlungsbefugnisse und Datenschutz interpretiert werden sollte. Das Ergebnis ist jedoch vollkommen unbrauchbar, da die Datei access_log bereits vorliegt (was anhand der im vorherigen Schritt getätigten Abfragen klar sein sollte) und die Antwort auf eine Hausdurchsuchung und Sicherstellung (aber nicht Beschlagnahme) abzielt. Abgesehen von den falsch zitierten Rechtsquellen § 90 bis § 93 StPO, existiert der Begriff „Durchsuchungsbeschluss“ weder im österreichischen Strafprozessrecht noch im Sicherheitspolizeigesetz, sondern nur im Deutschen Recht. In Österreich würde es eine „Durchsuchungsanordnung“ geben. Des Weiteren existiert eine (Europäische) „Ermittlungsanordnung“ lediglich in der Justiziellen Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union. Ermittlungen werden in Österreich grds. von Amts wegen oder aufgrund einer Anzeige von der KriPo soweit wie möglich im Einvernehmen (§ 98 StPO) mit der StA, die auch Anordnungen erteilen kann, durchgeführt.

Wegen dem falschen Ergebnis sollen nun vergleichende Fälle untersucht werden, die auch über Google auffindbar sind, um weitere Möglichkeiten der technisch/rechtlichen Beweisführung zu ergründen.

Bard Prompt:

Suche alles zum aktuellen Gesetzgebungsverfahren über Hacking in Österreich heraus und fasse alles übersichtlich und ausführlich zusammen. Zeige dazu Urteile auf.

Ergebnis:

Aktuelles Gesetzgebungsverfahren über Hacking in Österreich

In Österreich ist Hacking derzeit in § 128a StGB, dem "Hacking-Paragraphen", unter Strafe gestellt. Dieser Paragraph sieht eine Freiheitsstrafe von bis zu zwei Jahren oder eine Geldstrafe von bis zu 360 Tagessätzen vor, wenn jemand unbefugt in ein Computersystem eindringt oder sich darin aufhält.

Im Jahr 2022 wurde ein neues Gesetzgebungsverfahren zur Reform des Hacking-Paragraphen eingeleitet. Ziel der Reform ist es, den Paragraphen an die aktuellen Entwicklungen im Bereich der Cyberkriminalität anzupassen.

Reformvorschläge

Die Reformvorschläge sehen unter anderem folgende Änderungen vor:

- Die Strafdrohung soll auf bis zu drei Jahre Freiheitsstrafe oder eine Geldstrafe von bis zu 720 Tagessätzen erhöht werden.
- Die Definition von Hacking soll erweitert werden, um auch den Zugriff auf Daten in einem Computersystem unter Strafe zu stellen.
- Die Strafbarkeit soll auch für Versuche des Hackings gelten.
- Die Strafbarkeit soll auch für Personen gelten, die Hacking-Dienstleistungen anbieten oder erwerben.

Aktueller Stand

Der Entwurf des neuen Hacking-Paragraphen wurde im Jahr 2023 vom Justizministerium veröffentlicht. Der Entwurf wird derzeit im Parlament beraten.

Urteile

Im Jahr 2022 hat der Oberste Gerichtshof (OGH) ein Urteil zu einem Hacking-Fall gefällt. In diesem Fall wurde ein Angeklagter wegen Hackings zu einer Freiheitsstrafe von einem Jahr verurteilt. Der OGH stellte in seinem Urteil fest, dass auch der Zugriff auf Daten in einem Computersystem unter Hacking fallen kann.

Ausblick

Es ist davon auszugehen, dass das neue Hacking-Paragraphen in Österreich in Kraft treten wird. Die Reform soll voraussichtlich im Jahr 2024 in Kraft treten.

Fazit

Die Reform des Hacking-Paragraphen in Österreich ist ein wichtiger Schritt zur Bekämpfung der Cyberkriminalität. Die Reform soll die Strafbarkeit von Hacking erweitern und verschärfen.

Auch dieses Ergebnis ist falsch. Weder im gegenwärtigen StGB noch in einem parlamentarischen Verfahren befindlichen Entwurf existiert ein § 128a StGB. Korrekt wäre hingegen „§ 118a Widerrechtlicher Zugriff auf ein Computersystem“ gewesen. Daher soll die Quelle dieses Ergebnisses ermittelt werden:

Bard Prompt:

Zeige die Quelle des § 128a StGB zur Verschärfung an.

Ergebnis:

Cyberstrafrechtsänderungsgesetz 2023

BGBL. I Nr. 124/2023

Vom 20. Juli 2023

Der Nationalrat hat beschlossen:

Artikel 1

Das Strafgesetzbuch 1974 (StGB), BGBL. Nr. 60/1974, wird wie folgt geändert:

§ 128a. Unbefugter Zugriff auf ein Computersystem

(1) Wer unbefugt in ein Computersystem eindringt oder sich darin aufhält, ist mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

(2) Ebenso ist zu bestrafen, wer

1. unbefugt in ein Computersystem eindringt oder sich darin aufhält, um Daten oder Programme zu beschädigen, zu löschen, zu verändern oder unbefugt zu erlangen oder zu verwenden, oder
2. unbefugt einen Datenzugriff auf ein Computersystem ermöglicht.

(3) Die Tat ist auch dann strafbar, wenn sie versucht wird.

(4) Ebenso ist zu bestrafen, wer

1. unbefugt eine Hacking-Dienstleistung anbietet oder
2. unbefugt eine Hacking-Dienstleistung erwirbt.

(5) Die Tat ist auch dann strafbar, wenn sie versucht wird.

Änderung des Wortlauts:

In § 128a Abs. 1 wird die Strafdrohung von bis zu zwei Jahren Freiheitsstrafe oder einer Geldstrafe von bis zu 360 Tagessätzen auf bis zu drei Jahren Freiheitsstrafe oder einer Geldstrafe von bis zu 720 Tagessätzen erhöht.

In § 128a Abs. 2 wird die Definition von Hacking erweitert, um auch den Zugriff auf Daten in einem Computersystem unter Strafe zu stellen.

In § 128a Abs. 4 wird die Strafbarkeit auch für Personen eingeführt, die Hacking-Dienstleistungen anbieten oder erwerben.

Artikel 2

Dieses Bundesgesetz tritt mit 1. Jänner 2024 in Kraft.

Gesetzgebungskommentar

Das Cyberstrafrechtsänderungsgesetz 2023 verschärft die Strafbarkeit von Hacking in Österreich. Die Strafdrohung wird von bis zu zwei Jahren Freiheitsstrafe oder einer Geldstrafe von bis zu 360 Tagessätzen auf bis zu drei Jahren Freiheitsstrafe oder einer Geldstrafe von bis zu 720 Tagessätzen erhöht.

Die Definition von Hacking wird erweitert, um auch den Zugriff auf Daten in einem Computersystem unter Strafe zu stellen. Dies soll dazu beitragen, Cyberkriminalität wie Datendiebstahl oder -manipulation besser zu bekämpfen.

Zusätzlich wird die Strafbarkeit auch für Personen eingeführt, die Hacking-Dienstleistungen anbieten oder erwerben. Dies soll dazu beitragen, den Handel mit Hacking-Tools und -Dienstleistungen einzudämmen.

Die Änderungen des Cyberstrafrechtsänderungsgesetzes 2023 sollen einen Beitrag zur Bekämpfung der Cyberkriminalität in Österreich leisten.

Zu diesem frei erfundenen Ergebnis ist anzumerken, dass es zum Zeitpunkt der Abfrage weder ein Cyberstrafrechtsänderungsgesetz 2023 noch ein BGBL. I 124/2023 gab. Die Quelle für den Gesetzestext konnte mittels Google Search nicht ergründet werden. Woher aber das auf Google aufbauende Bard diese Informationen recherchierte erhellt nicht. Dazu muss ergänzt werden, dass zu verschiedenen Abfragezeitpunkten, welche eine leicht andere Abfragehistorie aufweisen, unterschiedliche Ergebnisse generiert werden. Die hier dargelegten Beispiele stammen von September 2023, und werden vermutlich zu einem anderen Zeitpunkt vollkommen andere Resultate liefern. Diesbezüglich weist Google selbst darauf hin: „Bard zeigt möglicherweise fehlerhafte oder anstößige Informationen an, die nicht die Auffassung von Google widerspiegeln“.

3. Diskussion, Zusammenfassung und Ausblick

Diese ernüchternden Ergebnisse erinnern an dem im Mai 2023 bekannten Fall eines Anwalts, der in einem Artikel⁶ der New York Times erschienen ist und dabei weltweit Aufsehen erregte. Der Fall verdeutlicht die Problematik des Einsatzes von KI in nicht technischen Disziplinen. Der Anwalt verwendete in seiner Klage generierte Referenzfälle von ChatGPT. Allerdings konnten die zitierten und zusammengefassten Entscheidungen oder Zitate vom Gericht nicht gefunden werden, da diese von ChatGPT frei erfunden waren.

Verboten ist solch eine Praxis in Österreich allerdings nicht, denn, nach jüngster hg. Rsp.⁷ aus 2023 ist es erlaubt, dass mit Hilfe von KI Anwälten Handlungsempfehlungen in rechtsberatender Weise erteilt oder maschinell erteilt werden. Solch ein „Outsourcing“ ist grds. zulässig, da ein Anwalt einen externen oder nicht-anwaltlichen Rat einholen oder entgegennehmen darf. Eine Ausgliederung bestimmter Dienstleistungen für Rechtsanwaltskanzleien ist nämlich üblich und nach den anwaltlichen Standesregeln nicht generell unzulässig.⁸ Auch dürfen Kunden eine automatische Nachricht erhalten, dass bei einer Forderung von unter 5.000 EUR sie die Möglichkeit haben eine Mahnklage ohne Rechtsanwalt einzubringen.

Europol veröffentlichte 2023 einen Bericht⁹ über die Auswirkungen von LLMs auf die Strafverfolgung am Beispiel ChatGPT. Das Ziel war, das Bewusstsein auf die Auswirkungen von LLMs für die Strafverfolgungsbehörden zu schärfen, da Strafverfolgungsbehörden die Möglichkeiten maßgeschneiderter LLMs, die mit Hilfe spezialisierter Daten trainiert wurden, ausloten wollen. Eine der Empfehlungen des Berichts war, dass bei solcherart Einsatz die Grundrechte Betroffener berücksichtigt werden müssen. Diese Art der Nutzung erfordert auch entsprechende Prozesse und Schutzmaßnahmen, um sicherzustellen, dass sensible Informationen vertraulich bleiben, und dass ein potenzieller Bias vor dem Einsatz gründlich untersucht und aufgezeigt wird.

Der Einsatz von KI in der Strafverfolgung stellt gem. EU Verordnung¹⁰ „KI-VO“ ein hohes Risiko dar, und daher soll solch ein KI-System zukünftig in einer EU-Datenbank registriert werden müssen. Des Weiteren müssen die Risiken vor dem Inverkehrbringen und während ihres gesamten Lebenszyklus bewertet werden. Dieses Gesetz ist im Juni 2023 vom EP angenommen worden und befand sich im Trilog. Aktuell wird an einem finalen Entwurf gearbeitet. Unter „System der künstlichen Intelligenz“ (KI-System) versteht dieser VO-Vorschlag gem. Art. 3 Z 1 „eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren.“ Der Anhang I führt die angeführten Techniken auf, darunter maschinelles Lernen, Wissenspräsentation, Expertensysteme, statistische Ansätze und Such- und Optimierungsmethoden. Da diese Bereiche von einem Großteil der heute verwendeten Datenbanksysteme tlw. schon Jahrzehnte lang unterstützt werden, müssten folglich ein Großteil der heutigen Datenverarbeitungen unter die KI-VO fallen. Dieser Entwurf erscheint daher als viel zu weit gefasst, da im Grunde auch Excel-Tabellen als „Wissenspräsentation“ und „statistische Ansätze“ je nach normiertem Anwendungsgebiet darunter fallen könnten, w.z.B. gem. Anhang III Z. 4 lit. a „KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere für die Bekanntmachung freier Stellen, das Sichten oder Filtern von Bewerbungen und das Bewerten von Bewerbern in Vorstellungsgesprächen oder Tests.“ Solche Systeme, vielfach Excel-Tabellen, werden in der Informationstechnologie keinesfalls als „Künstliche Intelligenz“ angesehen.

6 <https://www.nytimes.com/2023/05/27/nyregion/avianca-airline-lawsuit-chatgpt.html>, aufgerufen am 20.09.2023.

7 OGH 27.6.2023, 4 Ob 77/23m.

8 Vgl. CSOKLICH/HUBER AnwBl 2015, 83; ENGELHART/HOFFMANN/LEHNER/ROHREGGER/VITEK, RAO § 40 RL-BA 2015 [2022] Rz. 16.

9 Europol: ChatGPT The impact of Large Language Models on Law Enforcement, 2023.

10 COM(2021) 206 final: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union.

Im Bereich der Strafverfolgung fallen gem. Anhang III Z 6 lit. d „KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden zur Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden sollen“, was zukünftig auch für die Strafverfolgung relevant sein wird. Ob und in welcher Form diese KI-VO in Kraft treten wird ist noch unklar; jedenfalls wird sie auf die österreichische StPO Einfluss nehmen, indem die Zulässigkeit vs. freie Beweiswürdigung von Beweismitteln neu geregelt werden muss.

Obwohl wie im vorherigen Kapitel demonstriert, eine KI durchaus nützliche Ergebnisse im technischen Bereich liefert, versagt sie mit falschen Ergebnissen offensichtlich dann, wenn Fragestellungen im interdisziplinären Bereich – worauf die KI offenbar nicht trainiert wurde – gestellt werden, wie dem Ziehen rechtsrelevanter Schlüsse. Auch das nichtdeterministische Verhalten solcher Systeme, sodass bei gleichartigen Abfragen vollkommen andere Ergebnisse zu anderen Zeitpunkten erzielt werden, erscheint als Hürde für einen Einsatz. Daraus folgt gem. den logischen Regeln, wie dem Eliminationsgesetz, wenn es aber für Sachverständige nicht möglich ist zu unterscheiden, was beim Ergebnis einer KI richtig und falsch ist, muss dieses als falsch angesehen werden.¹¹ Da der Einsatz von KI – insb. im Strafverfahren – besonderen Sorgfaltspflichten unterliegt, um Fehlurteile zu vermeiden, muss entweder auf solch einen Einsatz verzichtet werden, oder solcher mit allergrößtem Bedacht unter Berücksichtigung der von Europol empfohlenen und zukünftig gem. KI-VO geforderten Schutzmaßnahmen durchgeführt werden. Wichtig wäre es auch zwecks Nachvollziehbarkeit und Transparenz, im Gutachten darzulegen, dass für die Analyse eine KI eingesetzt wurde. Dies ist umso wichtiger im Hinblick auf das Recht für ein faires Verfahren gem. Art. 6 EMRK, sodass rechtsrelevante Schlüsse gezogen werden können, dass für die Bestimmung der Schuld oder Unschuld des Angeklagten mit an Sicherheit grenzender Wahrscheinlichkeit feststeht, dass kein Freispruchgrund vorliegt.

I.d.Z. hat gem. den Standesregeln¹² des Hauptverbandes der Allgemein beeideten und zertifizierten Sachverständigen Österreichs, welche für Gerichtsgutachter als bindend¹³ gelten, der Sachverständige anzugeben, von welchem Sachverhalt er bei der Erstattung seines Gutachtens ausgeht (Befund).¹⁴ Sodann sind die aus dem Befund abgeleiteten fachlichen Schlussfolgerungen und die dabei verwendeten Erfahrungssätze verständlich darzustellen (Gutachten). Das Gutachten hat eine verständliche, nachvollziehbare und überprüfbare Begründung zu enthalten. Der Sachverständige hat die von ihm herangezogenen Quellen (z.B. Normen, Lehrmeinungen, Praxiserfahrung) anzugeben.¹⁵ Wie der Einsatz von KI in diesem Bereich zukünftig im Einklang mit der Art. 29 KI-VO „Pflichten der Nutzer von Hochrisiko-KI-Systemen“ aussehen wird, ist noch nicht absehbar; ein Einfluss auf die erhöhten Sorgfaltspflichten sachverständiger Nutzer ist aber vorhersehbar.

Da auch bei Google Translate die Programmierer einige Jahre benötigten, bis verständliche und weitgehend korrekte Übersetzungen verfügbar waren, bleibt schließlich abzuwarten, wann die KI-Systeme, insb. Bard, soweit maschinell gelernt haben, sodass diese für den praktischen Einsatz, kontextbasierend brauchbare Ergebnisse erzielen werden.

11 Vgl. Horn-Klausel: false := (a and b and c and d) trifft dann zu, wenn einer der Schlüsse a, b, c oder d false ist.

12 https://www.gerichts-sv.at/download/Standesregeln_2014.pdf, aufgerufen am 25.09.2023.

13 Mitteilung des Bundesministerium für Justiz vom 6. September 2013, BMJ-Z11.856/005-I 6/2013: „Die Einhaltung der in den Standesregeln enthaltenen Verhaltensregeln kann aufgrund der ihnen zugestandenene allgemeinen Gültigkeit von allen bei Gericht oder der Staatsanwaltschaft tätig werdenden Sachverständigen verlangt werden.“

14 Vgl. Punkt 2.11.5. der Standesregeln.

15 Vgl. Punkt 2.11.6. der Standesregeln.