Dr. Vyacheslav Bortnikov

KI IM STRAFVERFAHREN AUS DATENSCHUTZSICHT[1]

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung. Ich freue mich, das Thema ›KI im Strafverfahren – aus Datenschutzsicht‹ zu beleuchten.

Gleich zu Beginn möchte ich an die Frage anknüpfen, die beim diesjährigen Strafverteidigertag bereits mehrfach angeklungen ist »Wer kontrolliert den Einsatz von KI durch Strafverfolgungsbehörden?«. Das Bundesverfassungsgericht misst der Datenschutzkontrolle eine besondere Bedeutung zu, wenn Daten verdeckt verarbeitet werden, d.h. ohne dass betroffene Personen darüber informiert würden. Insofern obliegt der Datenschutzkontrolle eine ›Kompensationsfunktion‹, da subjektiver Rechtsschutz gegen derartige Maßnahmen nicht oder nicht ohne Weiteres zu erlangen ist.[2]

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – kurz BfDI – als die für die Polizei- und Strafverfolgungsbehörden des Bundes zuständige Datenschutzbehörde beschäftigt sich seit mehreren Jahren mit dem Einsatz von KI im Bereich der Strafverfolgung und der Gefahrenabwehr.[3] Bei meinem Vortrag werde ich einige Positionen des BfDI mit Bezug auf Strafverfolgungsbehörden vorstellen. Nach einer kurzen Einleitung werde ich insbesondere die Ergebnisse des Konsultationsverfahrens darstellen, das der

1 Der Beitrag entspricht im Wesentlichen einem Vortrag, den der Autor am 13. Mai 2023 auf dem 44. Strafverteidigertag gehalten hat. Der Vortragsstil wurde beibehalten. – Der Autor ist Regierungsdirektor bei dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

2 BVerfG, NJW 2016, 1781 Rn. 140 f.

3 Vgl. z.B. Symposium des BfDI vom 6.10.2021 ›Polizeiliche Informationssysteme im Zeitalter von KI und Big Data‹, https://www.bfdi.bund.de/SharedDocs/Videos/DE/Veranstaltungen/20211006_Symposium-KI-Polizei.html?nn=358604.

BfDI im Herbst 2021 zum Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr durchgeführt hat.[4] Schließlich werde ich das Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 zu automatisierter Datenanalyse erläutern und daraus mögliche Schlussfolgerungen für die praktische Rechtsanwendung ziehen.

A.

Einleitung

In meinem Vortrag geht es also um die Perspektive, in der die Sicherheitsbehörden selbst KI einsetzen wollen. Wir haben heute schon mehrfach gehört, dass Technologien, die unter dem Begriff KI firmieren, zunehmend Eingang in die Lebenswirklichkeit finden. Daher ist die Vermutung durchaus naheliegend, dass diese über kurz oder lang auch zu kriminellen Zwecken missbraucht werden.[5] Gleichzeitig steigen die Mengen an strafrechtlich relevanten Daten stetig an. Dass die Strafverfolgungsbehörden bei der technologischen Entwicklung nicht ins Hintertreffen geraten,[6] sondern auch selbst neue Technologien einsetzen wollen, ist vor diesem Hintergrund nachvollziehbar.

Das INTERPOL-Innovationszentrum hat KI als eine der Säulen der Innovation im Bereich der Strafverfolgung identifiziert.[7] Unter der Ägide des INTERPOL und des UN-Instituts für interregionale Kriminalitäts- und Justizforschung (UNICRI) fand im Juli 2018 das erste ›Global Meeting on Artificial Intelligence (AI) and Robotics for Law Enforcement‹ statt. Die Veranstaltung diente dazu, die Strafverfolgungsbehörden weltweit über KI und Robotik zu informieren, und als ein Forum zur Erörterung bewährter Praktiken in der Polizeiar-

4 https://www.bfdi.bund.de/DE/DerBfDI/Konsultationsverfahren/KI-Strafverfolgung/KI-Strafverfolgung_node.html.

5 Vgl. Stellungnahme des Bundesministeriums des Innern, für Bau und Heimat vom 29.11.2021, S. 2, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/2_KI-Strafverfolgung/Stellungnahmen/StgN-BMI.pdf?__blob=publicationFile&v=3.

6 UNICRI/INTERPOL, Artificial Intelligence and robotics for law enforcement, 2019, abrufbar unter: http://www.unicri.it/sites/default/files/2019-10/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB_0.pdf.

7 Interpol-Innovationszentrum, Artificial Intelligence: INTERPOL Innovation Centre's initiatives, S. 2. Abrufbar unter: https://www.interpol.int/en/content/download/17303/file/IC_APL%20AI%20Overview%20%28March%202022%29%20.pdf.

beit, aktuellen und künftigen Chancen und Bedrohungen sowie ethischen Herausforderungen, die sich aus dem Einsatz dieser Technologien ergeben.[8]

In dem entsprechenden Bericht wurde u.a. ausgeführt, dass viele Länder die Anwendung von KI und Robotik im Zusammenhang mit der Strafverfolgung erforschen, wobei einige Länder weiter seien als andere.[9] In dem Bericht wurden einige ›interessante‹ Beispiele für den Einsatz von KI und Robotern in der Strafverfolgung genannt:

- Vorhersage, wo und welche Art von Straftaten wahrscheinlich auftreten werden (›predictive policing‹ und ›crime hotspot analytics‹),
- Tools zur Identifizierung gefährdeter und ausgebeuteter Kinder,
- Vollautomatisierte Werkzeuge zur Identifizierung von Online-Betrügern.

Mehrere Anwendungsfälle im Bereich der Strafverfolgung seien in unterschiedlichen Entwicklungsstadien. Während einige sich noch in der Konzeptionierungsphase befinden würden, seien andere in der Evaluierungsphase oder bereits für den Einsatz zugelassen.[10]

Wie sieht die Situation in Deutschland aus?

Die vom BfDI in der Zeit vom 30. September bis zum 17. Dezember 2021 durchgeführte öffentliche Konsultation zum Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr hat gezeigt, dass der Einsatz von KI in bestimmten Phänomenbereichen gelebte Praxis darstellt. KI spielt naturgemäß vor allem bei der Auswertung großer Datenmengen eine wichtige Rolle. Der Gesamtdatenbestand der sog.

8 UNICRI/INTERPOL, Artificial Intelligence and robotics for law enforcement, 2019, S. III.; abrufbar unter: http://www.unicri.it/sites/default/files/2019-10/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB_0.pdf; Interpol-Innovationszentrum, Artificial Intelligence: INTERPOL Innovation Centre's initiatives, S. 3. Abrufbar unter: https://www.interpol.int/en/content/download/17303/file/IC_APL%20AI%20Overview%20%28March%202022%29%20.pdf.

9 UNICRI/INTERPOL, Artificial Intelligence and robotics for law enforcement, 2019, S. V.., abrufbar unter: http://www.unicri.it/sites/default/files/2019-10/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB_0.pdf.

10 UNICRI/INTERPOL, Artificial Intelligence and robotics for law enforcement, 2019, S. VI., abrufbar unter: http://www.unicri.it/sites/default/files/2019-10/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB_0.pdf.

›Panama Papers‹ belief sich laut Bundesministerium des Innern, für Bau und Heimat auf über 41,5 Mio. Datensätze und Dateiordner und wurde unter Zuhilfenahme eines neuronalen Netzes ausgewertet.[11] Weitere Einsatzbereiche seien alle Formen von Mustererkennungen (z. B. von Flaggen des sogenannten Islamischen Staates im Internet oder von sexuellen Missbrauchsdarstellungen von Kindern oder die Unschärfenbeseitigung in sichergestelltem Videomaterial).[12]

Ende Januar 2022 waren kritische Berichte über den Einsatz von KI durch die Sicherheitsbehörden des Bundes zu vernehmen. So hieß die Überschrift auf Zeit-Online vom 18. Januar 2022 »KI first, Bedenken second – Die Bundesregierung setzt auf künstliche Intelligenz, mehr als 80 staatliche Projekte laufen bereits. Die Risiken der Technik werden vorher offenbar kaum abgewogen«.[13] Das Portal Golem.de titelte am 26. Januar 2022 »Geheime KI ohne Risikoabschätzung bei Sicherheitsbehörden – Polizeien und Geheimdienste in Deutschland nutzen KI-Systeme. Wofür soll aber geheim bleiben. Eine Risikoabschätzung gibt es kaum«.[14]

Die zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) setzt nach eigenem Bekunden mehr und mehr Fokus auf KI.[15] Sie entwickle unter anderem ein selbstlernendes System, das den Strafverfolgern helfen soll, strafbare Social Media-Inhalte vorzusortieren.[16]

B.

11 Stellungnahme des Bundesministeriums des Innern, für Bau und Heimat vom 29.11.2021, S. 3, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/2_KI-Strafverfolgung/Stellungnahmen/StgN-BMI.pdf?__blob=publicationFile&v=3.

12 Stellungnahme des Bundesministeriums des Innern, für Bau und Heimat vom 29.11.2021, S. 3, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/2_KI-Strafverfolgung/Stellungnahmen/StgN-BMI.pdf?__blob=publicationFile&v=3.

13 https://www.zeit.de/digital/2022-01/url-kuenstliche-intelligenz-bundesregierung-risiken-enquete-kommission?utm_referrer=https%3A%2F%2Fwww.google.de%2F.

14 https://www.golem.de/news/kuenstliche-intelligenz-geheime-ki-ohne-risikoabschaetzung-bei-sicherheitsbehoerden-2201-162696.html.

15 https://www.behoerden-spiegel.de/2023/05/03/ki-fuer-die-strafverfolgungsbehoerden-braucht-mehr-trainingsdaten/.

16 https://www.behoerden-spiegel.de/2023/05/03/ki-fuer-die-strafverfolgungsbehoerden-braucht-mehr-trainingsdaten/.

Konsultationsverfahren des BfDI

Der Einsatz von KI wirft eine Reihe von Fragen auf. Um einen Beitrag zur öffentlichen Debatte zu leisten, hat der BfDI im Herbst 2021 folgende sieben Thesen zur Diskussion gestellt.

- KI erfordert eine ausführliche *empirische Bestandsaufnahme* und eine umfassende *gesellschaftspolitische Diskussion*, um einerseits die Auswirkungen dieser Technologie auf die Freiheiten der Bürgerinnen und Bürger zu klären und andererseits die Erforderlichkeit ihres Einsatzes zu Strafverfolgungs- und Gefahrenabwehrzwecken festzustellen. Die Risiken sind dem Nutzen umfassend gegenüberzustellen, etwaige Diskriminierungen und überindividuelle Folgen sowohl für bestimmte Personengruppen als auch für demokratische und rechtsstaatliche Abläufe insgesamt sind wirksam auszuschließen. Der Gesetzgeber ist gehalten, alle derzeit existierenden Befugnisse der Strafverfolgungs- und Gefahrenabwehrbehörden in eine Gesamtrechnung einzubeziehen (»Überwachungs-Gesamtrechnung«).
- Der Einsatz von KI kann *nicht auf polizeiliche Generalklauseln* gestützt werden. Vielmehr erfordert der Einsatz von KI grundsätzlich eine spezifische gesetzliche Regelung.
- Die Einhaltung der *allgemeinen Datenschutzgrundsätze* ist eine unabdingbare Voraussetzung für den datenschutzrechtlich zulässigen Einsatz von KI. Der Einsatz von KI darf ebenso eine effektive Ausübung der Betroffenenrechte nicht schmälern.
- KI muss *erklärbar* sein. Die Qualität der schon zu Trainingszwecken eingesetzten Datensätze ist sicherzustellen.
- Der Kernbereich privater Lebensgestaltung bzw. die *Menschenwürdegarantie* dürfen beim Einsatz von KI nicht tangiert werden.
- KI muss durch Datenschutzaufsichtsbehörden umfassend *kontrolliert* werden können.
- Dem Einsatz von KI muss eine umfassende *Datenschutzfolgen-Abschätzung* vorangehen.

C.

Urteil des BVerfG vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20

Am 16. Februar 2023 hat das Bundesverfassungsgericht ein Grundsatzurteil zu automatisierter Datenanalyse verkündet und damit verfassungsrechtliche Weichen auch für den Einsatz von KI gestellt.

I. Verfassungsrechtliche Einordnung

Bevor wir zum Kern der Entscheidung kommen, möchte ich das Urteil in die bisherige Rechtsprechung des Bundesverfassungsgerichts einordnen.

Das Bundesverfassungsgericht verbindet mit der elektronischen Datenverarbeitung eine gesteigerte Gefährdungslage.[17] Diese ist u.a. darauf zurückzuführen, dass personenbezogene Daten mittels elektronischer Datenverarbeitung unbegrenzt speicherbar und jederzeit und ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind.[18] »Sie können darüber hinaus mit anderen Datensammlungen zusammengefügt werden, wodurch vielfältige Nutzungs- und Verknüpfungsmöglichkeiten entstehen«.[19] Eine automatisierte Datenanalyse – insbesondere beim Einsatz von KI – kann die Erstellung von Bewegungs- und Verhaltens- oder Beziehungsprofilen oder noch umfassenderer Persönlichkeitsbilder ermöglichen, die so im Wege händischer Suche oder einfacher automatisierter Abgleiche nicht erlangt werden könnten.[20] Dies knüpft nahtlos an die seit dem Volkszählungsurteil bestehende Rechtsprechung an[21] und konkretisiert diese im Hinblick auf Datenanalysen.

II. Zentrale Aussagen aus dem Urteil

17 BVerfGE 120, 378 (397 f.).
18 BVerfGE 120, 378 (397 f.).
19 BVerfGE 120, 378 (398).
20 BVerfG, NJW 2023, 1196 Rn. 70.
21 BVerfGE 65, 1, (42 ff.).

Eine automatisierte Datenanalyse kann – fachlich und technisch – ganz unterschiedlich ausgestaltet sein. Je höher die Eingriffsintensität einer Datenanalyse im Einzelfall ist, desto höher sind die Anforderungen an ihre Rechtfertigung.[22] Diese Anforderungen betreffen vor allem die Eingriffsschwelle, das zu schützende Rechtsgut, die Sicherung von Transparenz, Rechtsschutz und aufsichtlicher Kontrolle. Ist die Eingriffsschwelle niedrig, weil die Datenanalyse z.B. bereits im Vorfeld einer konkreten Gefahr oder zur vorbeugenden Bekämpfung einer Straftat eingesetzt wird, muss das zu schützende Rechtsgut entsprechend höher sein.[23]

Was beeinflusst die Eingriffsintensität einer automatisierten Datenanalyse?

Maßgebliche Bedeutung kommt damit den Faktoren zu, die das Eingriffsgewicht einer automatisierten Datenanalyse beeinflussen. Insofern kommt es in dem hier relevanten Kontext insbesondere auf die *Art und Umfang der Daten* sowie auf die *Verarbeitungsmethoden* an. Künstliche Intelligenz im Sinne eines selbstlernenden Systems stellt in diesem Sinne eine Verarbeitungsmethode bzw. eine Methode der automatisierten Datenanalyse dar, deren Verwendung je nach Einsatzart ein besonderes Eingriffsgewicht haben kann.[24] Die spezifischen Gefahren der Verwendung von KI sieht das Bundesverfassungsgericht darin,

> »dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden. Mittels einer automatisierten Anwendung könnten so über den Einsatz komplexer Algorithmen zum Ausweis von Beziehungen oder Zusammenhängen hinaus auch selbstständig weitere Aussagen im Sinne eines ›predictive policing‹ getroffen werden. So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert

22 BVerfG, NJW 2023, 1196 Rn. 71 ff.

23 BVerfG, NJW 2023, 1196 Rn. 74, 103 ff.

24 BVerfG, NJW 2023, 1196 Rn. 100.

sein kann. Denn komplexe algorithmische Systeme könnten sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein«.[25]

Will der Gesetzgeber die Eingriffsintensität einer automatisierten Datenanalyse reduzieren, muss er dafür den Einsatz selbstlernender Systeme im Gesetz ausdrücklich ausschließen.[26]

Es besteht die Gefahr, dass sich diskriminierende Algorithmen herausbilden und diese in der Praxis verwendet werden. Vor diesem Hintergrund hat das Bundesverfassungsgericht für die Anwendung von KI in der Polizeiarbeit im Urteil vom 16. Februar 2023 klare Worte gefunden: selbstlernende Systeme dürfen in der Polizeiarbeit »nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern.«[27]

Weitere Kriterien, die sich auf die Eingriffsintensität auswirken, sind u.a.:

- Grad der Automatisierung;
- Einsatz von Software privater Akteure oder anderer Staaten;
- denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs;
- Fehler- und Diskriminierungsanfälligkeit des eingesetzten Datenanalysetools;
- Verknüpfung mit dem Internet;
- Zahl und Qualifikation der Personen, die Zugriff auf das Analyseinstrument haben.

III. Schlussfolgerungen aus dem Urteil für die

25 BVerfG, NJW 2023, 1196 Rn. 100.
26 BVerfG, NJW 2023, 1196 Rn. 120 f.
27 BVerfG, NJW 2023, 1196 Rn. 100.

PRAKTISCHE RECHTSANWENDUNG

Welche Schlussfolgerungen lassen sich daraus für die praktische Rechtsanwendung ableiten?

Je nach Grundrechtssensibilität ist die Frage zu klären, ob die für die automatisierte Datenanalyse herangezogenen Rechtsgrundlagen dafür tauglich sind. Sollte dies nicht der Fall sein, ist die mit der Datenanalyse verbundene Datenverarbeitung rechtswidrig.

Ein anschauliches Beispiel dafür, wie eine verfassungskonforme (enge) Auslegung in der Praxis vorgenommen werden kann, bildet der Beschluss des LG Frankfurt (Oder) vom 22.07.2022 – 22 Os 40/19. Das LG beschloss, dass der Betrieb eines Kennzeichenerfassungssystems im Aufzeichnungsmodus rechtswidrig war. Die zum Einsatzzeitpunkt vorhandenen Rechtsgrundlagen hat das LG insbesondere wegen der verfassungsrechtlichen Dimension als nicht tauglich erachtet.[28] Aufgrund ihrer hohen Grundrechtssensibilität konnte die Maßnahme nicht auf § 100h Abs. 1 StPO gestützt werden, da diese Norm keine hinreichenden Begrenzungen, etwa in räumlicher Hinsicht, insbesondere jedoch keine ausreichenden prozessualen Verfahrenssicherungen aufweist;[29] »es fehlte an Regelungen zur Datenspeicherung, -löschung und -sicherheit sowie den Zugriffsmöglichkeiten, einem effektiven Richtervorbehalt, und an der Gewährleistung effektiven individuellen Rechtsschutzes und hinreichender Transparenz«.[30] »Es hätte vielmehr spezieller auf die automatische Kennzeichenerfassung zugeschnittener Ermächtigungsgrundlagen (mit verschärften Voraussetzungen und höherer Regelungsdichte) bedurft«[31], die zum Zeitpunkt der verfahrensgegenständlichen Datenverarbeitungen jedoch nicht vorlagen.

28 Vgl. LG Frankfurt (Oder), BeckRS 2022, 19483, insbes. Rn. 61 ff.

29 LG Frankfurt (Oder), BeckRS 2022, 19483, Rn.70.

30 LG Frankfurt (Oder), BeckRS 2022, 19483, Rn.70.

31 LG Frankfurt (Oder), BeckRS 2022, 19483, Rn. 69.

D.
AUSBLICK

Meine Damen und Herren,

das Thema KI wird ein ständiger Begleiter auch in der Praxis der Justiz- und Datenschutzbehörden sein. Deshalb freue ich mich auf den weiteren Fachaustausch. Bei der Gelegenheit möchte ich Sie auf das am 26. Oktober 2023 anstehende Symposium des BfDI unter dem Titel ›Automatisierte Datenanalyse und KI - Innovative Polizeiarbeit mit Diskriminierungspotenzial?‹ hinweisen. Weitere Informationen finden Sie zu gegebener Zeit auf der Webseite www.bfdi.bund.de.