

# Exposé

zur Dissertation mit dem Arbeitstitel

## Künstliche Intelligenz in der Strafverfolgung

### Einsatzmöglichkeiten in der Verbrechensbekämpfung und -prävention

#### 1. Einführung

In den 1970er Jahren setzte still eine der größten Revolutionen ein, die die Welt jemals gesehen hatte; nachdem man rund 100 Jahre zuvor gelernt hatte, Elektrizität zu produzieren und sich zu Nutze zu machen, fanden erstmals graue box-förmige Rechenmaschinen ihren Weg in die Privathaushalte; der „PC“ als „Personal Computer“ war geboren und löste eine Entwicklungswelle aus, deren Ausmaß selbst in den mutigsten Zukunftsprognosen niemals vorhergesehen hätte werden können. In rasantem Tempo wurde unsere Welt von einer analogen in eine digitale transformiert und unser Alltag von Grund auf verändert. Diese digitale Revolution hat eine neue Revolution angestoßen, deren Namen man nun auch in der breiteren Öffentlichkeit wahrzunehmen beginnt. Dem Begriff „künstliche Intelligenz“ (gerne auch in seinem englischem Counterpart „Artificial Intelligence“) begegnet man inzwischen nämlich nicht mehr nur als Plot-Point in Science-Fiction Romanen und Hollywood-Filmen, sondern als ernstzunehmende Technologien, die enormes Potential haben, unsere Welt ein weiteres Mal komplett zu transformieren.

Wenn man ein wenig unter die Oberfläche blickt, offenbart sich schnell, dass künstliche Intelligenz als Technologie nicht nur die Basis für die nächste „Tech-Bubble“ ist, die die IT-Branche in Silicon Valley euphorisch anpreist, sondern bereits jetzt zu tiefgehenden Veränderungen in einer Vielzahl von Wirtschaftsbereichen geführt hat.<sup>1</sup> Inzwischen haben KI-Systeme sich so weit entwickelt, dass die meisten von uns bereits ohne es zu wissen, jeden Tag mit diesen in Kontakt kommen; bei der Verwendung von Google, Netflix oder verschiedenen sozialen Medien laufen z.B. Image-Filter und Nutzungs-Optimierungssysteme im Hintergrund, die individuell auf uns zugeschnittene Kontaktvorschläge machen, uns besonders interessante Inhalte und Werbungen zeigen und für uns uninteressante Angebote ausblenden sollen<sup>2</sup>. KI wird inzwischen aber etwa auch von Bank- und Kreditinstituten bei der Kreditvergabe eingesetzt, sei es zur Aussonderung von nicht kreditwürdigen Klienten oder um aus Abermillionen tagtäglicher Bankbewegungen auffällige – etwa Geldwäsche-verdächtige -, Transaktionen herauszufiltern und zu melden, um nur einige Beispiele zu nennen.<sup>3,4</sup>

Schätzungen gehen davon aus, dass in den kommenden Jahren zwischen 20% - 26% aller Jobs von gravierenden Veränderungen durch den Einsatz von KI-Systemen betroffen sein werden.<sup>5</sup> Die Ausgaben für KI-Technologien in Europa verzeichneten allein im Jahr 2019 ein Wachstum von 49% im Vergleich zum Jahr 2018 (und erreichten damit eine Summe von rund USD 5,2 Milliarden).<sup>6</sup> Experten erwarten eine zunehmende Adoption von KI-Technologien auf wirtschaftlicher und gesellschaftlicher Ebene und prognostizieren eine rasante technologische Weiterentwicklung; so geht die Mehrheit einschlägig tätiger Wissenschaftler in einer Umfrage davon aus, dass KI-Systeme bis ca. zum Jahr 2050, menschenähnliche Intelligenz und Fähigkeiten entwickelt haben werden.<sup>7</sup>

Doch der Einsatz von KI-Technologien bringt nicht nur enorme Chancen, sondern auch gravierende Risiken mit sich.<sup>8</sup> So wird in Expertenkreisen längst über die weitere Entwicklung von KI und die mit ihrem Einsatz

---

<sup>1</sup> Vgl. DUAN/EDWARDS/DWIVEDI, Artificial intelligence for decision making in the era of Big Data, in: International Journal of Information Management 48 (2019), S. 63, mwN.

<sup>2</sup> RUEP, Schutzzonen für das Menschliche trotz künstlicher Intelligenz, in: derStandard (online), 03.02.2020 (<https://www.derstandard.at/story/2000113987689/schutzzonen-fuer-das-menschliche-trotz-kuenstlicher-intelligenz>; Zugriff 16.05.2020).

<sup>3</sup> DELOITTE, The case for artificial intelligence in combating money laundering and terrorist financing, Deloitte white paper (2018), S. 8f (<https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/finance/sea-fas-deloitte-uob-whitepaper-digital.pdf>; Zugriff am 07.04.2020).

<sup>4</sup> KINGDON, AI Fights Money Laundering, the IEEE Computer Society (2004), (<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1315546>; Zugriff am 07.04.2020).

<sup>5</sup> Ebenda.

<sup>6</sup> INTERNATIONAL DATA CORPORATION (IDC): Automation and Customer Experience Needs Will Drive AI Investment to \$5 Billion by 2019 Across European Industries (2019) (<https://www.idc.com/getdoc.jsp?containerId=prEMEA44978619>; Zugriff am 09.04.2020), vgl. in: DWIVEDI/HUGHES u.a., Artificial Intelligence (AI): Multidisciplinary perspectives, in: International Journal of Information Management (2019) (in press), S. 2.

<sup>7</sup> MÜLLER/BOSTROM, Future Progress in Artificial Intelligence, in: AI Matters (2014), S. 9.

<sup>8</sup> RUEP, Schutzzonen für das Menschliche trotz künstlicher Intelligenz, in: der Standard (online), 03.02.2020 (<https://www.derstandard.at/story/2000113987689/schutzzonen-fuer-das-menschliche-trotz-kuenstlicher-intelligenz>; Zugriff 16.05.2020).

verbundenen gesellschaftlichen, rechtlichen, wirtschaftlichen und ethischen Konsequenzen diskutiert; wobei nicht übersehen werden darf, dass die Entwicklung von KI selbst oft losgelöst von der Diskussion über ihre allfälligen erwünschten Fähigkeiten und unerwünschten Nebenwirkungen rasant weiterläuft und die Debatte darüber, was KI in Zukunft können soll oder können darf, daher dem tatsächlichen technischen Fortschritt oft beträchtlich hinterherhinkt.<sup>9</sup> Aber nicht nur akademische Fachkreise kommen der technischen Entwicklungen teils kaum mehr hinterher, sondern zeigt sich eine noch viel gravierendere Zeitverzögerung zwischen dem technischen Fortschritt und einem Aktivwerden der Politik in Hinblick auf Regulierung und Kontrolle einerseits,<sup>10,11</sup> aber auch in Rücksicht auf Rezeption und Förderung dieser Technologien andererseits.<sup>12</sup>

Unabhängig davon, was man von solchen Entwicklungen hält und wie skeptisch man diesen gegenübersteht, ist es nicht mehr zu leugnen, dass „intelligente“ Maschinen unaufhaltsam unsere Welt erobern. Deren zukünftiger Einsatzbereich wird sich dabei bei Weitem nicht auf Verbesserung von Google-Suchen und Serienempfehlungen von Netflix beschränken, sondern auch sehr sensible Lebensbereiche berühren, wie zum Beispiel die Bereiche der öffentlichen Sicherheit und der Rechtspflege.

KI-Technologien bieten dabei den Strafverfolgungsbehörden noch nie dagewesene Möglichkeiten der Prävention, Überwachung und Verfolgung von Verbrechen und sind die Einsatzgebiete breitgefächert; vom Einsatz beim „Urban Policing“, um etwa Fahrgäste des öffentlichen Nahverkehrs besser davor zu schützen, einem Verbrechen zum Opfer zu fallen,<sup>13</sup> über den Einsatz bei Risikoanalysen zur frühzeitigen „Gefährder-Erkennung“ oder der Verwendung künstlicher Intelligenz zur effizienteren Beweissammlung im Ermittlungsverfahren, bis hin zur Implementierung von KI-Systemen als Entscheidungshilfe im Hauptverfahren selbst.

Ebenso vielfältig wie die Einsatzbereiche sind aber auch die Probleme, die sich ergeben können. Das Risiko, dass es zu falschen, unfairen und intransparenten Entscheidungen kommt, ist selbst bei Vorliegen der besten Intentionen seitens Entwickler und Anwender und einwandfrei funktionierender Technik nicht zu unterschätzen.

Und während KI selbst grundsätzlich als „value neutral“ beschrieben werden kann, der Einsatz dieser Technologien also weder an sich „böser“ noch gutartiger Natur ist, sondern es alleine auf den Anwender und dessen Motive, sowie auf die Rahmenbedingungen der Anwendung ankommt,<sup>14</sup> wirft die potentielle Macht, die diese neuen Technologien mit sich bringen kann, gesellschaftlich enorm wichtige Fragen auf, wie etwa die Frage, in welcher Gesellschaft wir in Zukunft leben wollen und wie viel uns Sicherheit wert ist in Abwägung zu Freiheit? Derartige Fragen mögen anfangs überzogen wirken, erfahren aber schnell mehr Berechtigung, sobald man sich in anderen Ländern, in denen diese neuartigen Technologien bereits weit stärker rezipiert wurden, umsieht.<sup>15</sup> Insbesondere in China, dem absoluten Spitzenreiter in Sachen Überwachung, erreicht der Einsatz von KI-unterstützten Technologien inzwischen ein geradezu dystopisches Ausmaß. Betrachtet man die Auswirkungen dieses umfassenden Einsatzes, ergibt sich ein erschreckendes Bild davon, wie unser Alltag aussehen könnte, wenn derartig mächtige Technologien außerhalb straffer rechtlicher Regulatorien und außerhalb der engen Grenzen, die von starken menschen- und grundrechtlichen Überlegungen abgesteckt werden, zum Einsatz kommen.<sup>16</sup>

Die Überwachung der chinesischen Bürger ist inzwischen nahezu lückenlos; fast jeder Schritt wird von vernetzten Überwachungskameras getrackt; will man ein Ticket eines öffentlichen Verkehrsmittels kaufen oder entwerfen, so werden die Daten und das Gesicht des Käufers binnen eines Augenblicks mit Datenbanken abgeglichen, jede Äußerung in sozialen Medien oder im sozialen Umfeld wird mitgelesen oder nach Meldung registriert. In diesem Netz verfangen sich neben bekannten Regime-Kritikern auch schon viele zuvor unbescholtene Bürger, die die

<sup>9</sup> NUNN, When Superman Used X-Ray Vision, Did He Have a Search Warrant? in: Journal of Urban Technology, (2002), S. 70.

<sup>10</sup> PAPPAS/MIKALEF u.a., Big data and business analytics ecosystems, in: Information Systems and e-Business Management, 16:3 (2018), S. 481 u 489.

<sup>11</sup> DWIVEDI/HUGHES u.a., Artificial Intelligence (AI): Multidisciplinary perspectives, in: International Journal of Information Management (2019) (in press), S. 2.

<sup>12</sup> DJEFALL, Normative Leitlinien für künstliche Intelligenz in Regierung und öffentlicher Verwaltung, (2018), S. 494.

<sup>13</sup> Vgl. KOUZIOKAS, The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment, in: Transportation Research Procedia 24 (2017) S. 467–473.

<sup>14</sup> FELDSTEIN, Steven, The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, 17.09.2019 (<https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>; Zugriff am 24.05.2020).

<sup>15</sup> Wobei selbstverständlich auch sehr positive Beispiele des Einsatzes von KI gefunden werden, wie auch in den folgenden Punkten noch zu sehen sein wird.

<sup>16</sup> CAMPBELL, The Entire System Is Designed to Suppress Us, in: Time Magazine (Online), 21.11.2019 (<https://time.com/5735411/china-surveillance-privacy-issues/>; Zugriff am 24.05.2020).

chinesische Regierung als „unbequem“ oder „gefährlich“ einstufte, eine Vielzahl davon etwa in den uigurischen Provinzen Chinas, die aufgrund ihres muslimischen Glaubens unter Generalverdacht der Regierung gerieten. So reichte es in einigen Fällen aus, sich unter dem ständig wachsenden Augen der Kameras einen Bart wachsen zu lassen, sich durch die Hintertür aus dem Haus zu begeben oder eine Moschee zu besuchen, um die Alarmglocken der Algorithmen auszulösen und festgenommen zu werden.<sup>17</sup> In den von der UN seit Jahren angeprangerten und von China euphemistisch als „Umerziehungslager“ bezeichneten Festhaltezentren, finden sich daher hinreichend viele Menschen, die aufgrund der KI-unterstützt gesammelten Daten angeklagt und verurteilt wurden.<sup>18</sup>

Selbstverständlich trennt nun Österreich und China weit mehr als nur das Level an KI, das seitens des Staates eingesetzt wird, dennoch lässt sich bei näherer Betrachtung nicht mehr leugnen, dass mit dem raschen Fortschritt der künstlichen Intelligenz die oben gestellten Fragen immer drängender nach einer Antwort, oder zumindest nach dem Beginn einer tiefgreifenden gesellschaftsweiten Diskussion verlangen.

Es wird daher zu untersuchen sein, ob und inwieweit Instrumente, die auf künstlicher Intelligenz basieren, überhaupt im (österreichischen) Strafrecht Platz finden und mit den vorherrschenden Prinzipien wie etwa dem Rechtsstaatsprinzip in Einklang gebracht werden können. Die geplante Dissertation zielt daher darauf ab, diesen Fragen auf den Grund gehen und mitzuhelfen, ein Verständnis für künstliche Intelligenz selbst, aber auch für die Chancen und Risiken, die ihr Einsatz im Bereich der Strafverfolgung allfällig mit sich bringen kann, zu schaffen.

## 2. Strukturelle Gliederung und Forschungsschwerpunkt

Im folgenden Abschnitt soll ein kurzer Überblick über die Forschungsschwerpunkt gegeben werden, sowie der Begriff „künstliche Intelligenz“ kurz erläutert werden.

### 2.1. Was ist künstliche Intelligenz?

Während der Begriff „künstliche Intelligenz“<sup>19</sup> uns in den Medien mit rasch zunehmender Frequenz begegnet und inzwischen wohl jedermann meint, sich zumindest annähernd etwas darunter vorstellen zu können, mag es überraschen, dass sich hinter diesem Überbegriff keine auch nur annähernd einheitliche Definition verbirgt, sondern der Begriff „künstliche Intelligenz“ lediglich ein sich stetig wandelndes Konzept zu umschreiben vermag.<sup>20</sup> Eine schöne Annäherung liefert die Umschreibung als „Fähigkeit einer Maschine durch Erfahrung zu lernen, sich entsprechend auf neue Inputs einzustellen und einem Menschen ähnlich, Aufgaben zu erfüllen“.<sup>21</sup> Russell und Norvig hingegen beschreiben künstliche Intelligenz, als „ein System, das in der Lage ist, kognitive Funktionen, die grundsätzlich mit menschlichen Attributen verbunden sind, wie etwa Lernen, Sprache oder Problemlösung nachzuahmen“.<sup>22</sup> Kaplan und Haenlein definieren KI über ihre „Fähigkeit, unabhängig externe Datensätze zu interpretieren, aus diesen zu lernen und darauf aufbauend, bestimmte Ziele mittels flexibler Adaption zu erreichen“.<sup>23</sup> Der rote Faden, der sich durch all diese Definitionen zieht, ist die zunehmende Fähigkeit von Maschinen, Aufgaben, die derzeit noch von Menschen ausgeführt werden, zu übernehmen, wobei sie in einigen dieser Aufgabenbereichen bereits in der Lage sind, im Vergleich zum menschlichen Counterpart, Resultate von überragender Qualität zu liefern.<sup>24</sup>

---

<sup>17</sup> Ebenda.

<sup>18</sup> Ebenda.

<sup>19</sup> Beziehungsweise engl.: „artificial intelligence“, abgekürzt als „AI“.

<sup>20</sup> DUAN/EDWARDS/DWIVEDI, Artificial intelligence for decision making in the era of Big Data, in: International Journal of Information Management 48 (2019), S. 63 u. 67.

<sup>21</sup> DUAN/EDWARDS/DWIVEDI, Artificial intelligence for decision making in the era of Big Data, in: International Journal of Information Management 48 (2019), S. 63.

<sup>22</sup> Russell and Norvig definierten den Begriff „künstliche Intelligenz“ als: „systems that mimic cognitive functions generally associated with human attributes such as learning, speech and problem solving“ (in: DWIVEDI/HUGHES u.a., Artificial Intelligence (AI): Multidisciplinary perspectives, in: International Journal of Information Management (2019) (in press), S. 2).

<sup>23</sup> KAPLAN/HAENLEIN, Siri, Siri, in My Hand: Who's the Fairest in the Land? in: Business Horizons 62:1 (2019), S. 17.

<sup>24</sup> So zeigt sich etwa enormes Potenzial beispielsweise bei der Diagnose von Krebserkrankungen, vgl. HUANG/YANG u.a., Artificial intelligence in cancer diagnosis and prognosis, in Cancer Letters 471 (2020), S. 61–71.

Dies zeigt sich etwa insbesondere im Zusammenhang mit dem Aufkommen moderner Datenmanagement-Technologien (Schlagwort: „Big Data“<sup>25</sup> und „Data Mining“<sup>26</sup>), welche zu einem neuerlichen Innovationsschwingung im KI-Bereich geführt haben.<sup>27</sup> Durch Maschinen mit massiv verbesserten Speicherkapazitäten, die blitzschnell in der Lage sind, riesige Datenmengen zu prozessieren, können diese Massen an Informationsteilchen, einer KI-unterstützten Analyse zu Grunde gelegt werden, welche es ermöglicht, Verbindungen aufzuzeigen, die vorher unentdeckt geblieben wären oder Muster zu erkennen, die ein menschlicher Anwender niemals identifizieren hätte können und bieten diese Technologien zB im Bereich der Beweissammlung im Ermittlungsverfahren enormes Potential für Strafverfolgungsbehörden.<sup>28</sup>

## 2.2. Einsatz künstlicher Intelligenz zur Verbrechensprävention

Viele Polizeibehörden sehen sich zunehmend einem Dilemma ausgesetzt, da sie einerseits mit schrumpfenden Budgets und Personalmangel zu kämpfen haben, sich andererseits aber einem wachsenden Druck seitens der Medien und der Öffentlichkeit ausgesetzt sehen, die (natürlich nicht zu Unrecht) eine effektive und effiziente Polizeiarbeit einfordert.<sup>29</sup> Spätestens seit den Ereignissen des 11. September 2001, wurde die öffentliche Sicherheit auf politischer Ebene ein immer wichtigeres Gut und fordert die Gesellschaft auf nationaler wie auch auf globaler Ebene die Gewährleistung eines hohen Sicherheitslevels viel stärker ein.<sup>30</sup> Neben diesem wachsenden politischen und medialen Druck, möglichst von Jahr zu Jahr sinkende Kriminalitätsraten und steigende Aufklärungszahlen präsentieren zu können, hat sich aber auch das Arbeitsfeld der Strafverfolgungsbehörden um neue Kriminalitätsformen erweitert<sup>31</sup> und sich die Verbrechensbegehung globalisiert.

Um einen Ausweg aus diesem Dilemma zu finden, bieten KI-gestützte Technologien attraktive Lösungsansätze; da abgesehen von den eingangs notwendigen Investitionen zum Aufbau der KI-Strukturen und der Schulung des Personals,<sup>32</sup> KI-Systeme auf Dauer erheblichen Personalaufwand einsparen können und die laufenden Kosten im Vergleich zu Strukturen, die auf dem Einsatz von menschlichen Akteuren aufbauen müssen, wesentlich geringer sind.

Das eingangs geschilderte Dilemma erschöpft sich aber eben nicht nur in den budgetären Restriktionen, die es zu überkommen gilt, sondern auch darin, dass trotz sinkender Geldmittel, der „Output“ - also die Effektivität der Strafverfolgung -, gewährleistet oder möglichst sogar verbessert werden muss. Hier war lange Zeit einer der Knackpunkte, an der der breitgefächerte Einsatz bzw. zumindest die breitaufgestellte Testung von KI-Systemen im Strafverfolgungsbereich scheiterte: der Output konnte nicht stabil genug jene Ergebnisqualität liefern, die erforderlich wäre, um KI-Systeme im Praxis-Alltag einzusetzen bzw. zu testen.

Sinkende Kosten für die initiale Investition und technologische Fortschritte etwa im Bereich von „Predictive Analytics“, Sprach- und Gesichtserkennung, sowie die Verfügbarkeit erheblich besserer Datenmanagement Technologien („Big Data“), lassen die auf dem Markt angebotenen KI-Systeme jedoch zunehmend auch für die Strafverfolgungsbehörden attraktiv werden. Wirft man einen Blick auf andere Länder, so finden sich bereits einige Beispiele, in welchen die nationalen Strafverfolgungsbehörden, KI-unterstützte Systeme bei der Verbrechensbekämpfung und im Bereich der Verbrechensprävention einsetzen. Neben China zeigt sich hier

---

<sup>25</sup> Auch dieser Begriff verfügt über keine einheitliche Definition; bspw. CHEN/SHIWEN/YUNHAO geben dazu folgende generelle Definition an: „In general, big data shall mean the datasets that could not be perceived, acquired, managed, and processed by traditional IT and software/hardware tools within a tolerable time.“ (vgl. CHEN/SHIWEN/YUNHAO, Big data, in: Mobile networks and applications 19:2 (2014), S. 173).

<sup>26</sup> Ähnlich wie bei „Big Data“ gilt auch hier, dass es ein Vielfaches verschiedener Definitionen gibt; „Data mining“ kann aber generell wie folgt definiert werden: „Data mining is a process for extracting hidden, unknown, but potentially useful information and knowledge from massive, incomplete, noisy, fuzzy, and random data (vgl. CHEN/SHIWEN/YUNHAO, Big data, in: Mobile networks and applications 19:2 (2014), S. 191).

<sup>27</sup> DUAN/EDWARDS/DWIVEDI, Artificial intelligence for decision making in the era of Big Data, in: International Journal of Information Management 48 (2019), S. 63.

<sup>28</sup> WATKINS/REYNOLDS u.a., Tracking dirty proceeds, in: Police Practice and Research, 4:2 (2003), S. 163; S. 169f.

<sup>29</sup> Vgl. CENTRE FOR PUBLIC IMPACT, Durham Constabulary's AI decision aid for custody officers (2018), S. 2.

<sup>30</sup> NUNN, When Superman Used X-Ray Vision, Did He Have a Search Warrant? in: Journal of Urban Technology (2002), S. 69f.

<sup>31</sup> Die steigende Effizienz und vereinfachte Bedienbarkeit dieser Technologien lockt inzwischen auch immer mehr Kriminelle an und lässt eine neue Art der Kriminalität entstehen („Artificial Intelligence Crime“; etwa automatisierte Formen von Betrug, die sich hauptsächlich auf soziale Medien konzentrieren, und sich KI-unterstützt, das vergangene Userverhalten zu Nutzen machen um ihn gezielt anzusprechen, vgl. KING/AGGARWAL u.a., Artificial Intelligence Crime, in: Science and Engineering Ethics 26 (2020), S. 89f und 90.

<sup>32</sup> Kosten, die bis vor kurzem zugegebenermaßen oft noch abschreckend hoch waren, inzw. aber erheblich gesunken sind.

insbesondere der anglo-amerikanische Raum – wie so oft bei neuentwickelten Technologien – als „Early Adopter“ und Vorreiter.

So testeten z.B. die lokalen Polizeibehörden im britischen Durham bereits beginnend im Jahr 2013 eine KI-Anwendung („Harm Assessment Risk Tool“, „HART“), welche bei der Entscheidung über Entlassungen von Häftlingen, die sich in Untersuchungshaft befanden, eingesetzt werden sollte.<sup>33,34</sup> Zur Vorbereitung wurden dazu Basisdaten, bestehend aus 34 verschiedenen Kategorien - von Alter bis hin zur bisherigen Straffälligkeit- von den U-Häftlingen aus den vergangenen 5 Jahren erhoben und in ein System eingespeist, wobei auch Daten über vorherige Rückfälle nach einer Haftentlassung innerhalb dieses Zeitraumes enthalten waren.<sup>35</sup> Das System stufte sodann jeden U-Häftling in eine von drei Gruppen ein, und zwar in „geringes Risiko“, „mittleres Risiko“ oder aber „hohes Risiko“, je nachdem für wie wahrscheinlich die Anwendung es anhand der verfügbaren Daten hielt, dass der jeweilige U-Häftling nach seiner Entlassung wieder ein Verbrechen begehen würde.<sup>36</sup> Die Resultate – also ob die U-Häftlinge nach ihrer Entlassung tatsächlich rückfällig wurden oder nicht – wurden dann über zwei Jahre gesammelt und ausgewertet. Im Ergebnis zeigte sich im Rahmen dieses Tests, dass die Zuordnung von U-Häftlingen zur „geringes Risiko“-Gruppe in 98% der Fälle zutreffend gewesen war, während die Klassifizierung „hohes Risiko“ in 88% aller Fälle korrekt einen Rückfall vorhergesagt hatte.

Dieses Ergebnis reflektiert dabei aber auch eines der Probleme mit derartigen Prognoseinstrumenten; die HART-Anwendung zeigte eine Prädisposition, Häftlinge eher der Gruppe „mittleres Risiko“ oder „hohes Risiko“ zuzuordnen, als der Geringrisiko-Gruppe und somit eher auf Seiten der Vorsicht zu irren, als einen U-Häftling fälschlicherweise als wenig rückfallsgefährdet zu klassifizieren und damit unter Umständen einen gefährlichen Straftäter frühzeitig zu entlassen.<sup>37</sup> Während der laufenden Testphase wurde die Treffsicherheit der HART-Anwendung regelmäßig evaluiert, wurde zu diesem Zeitpunkt aber laut der Behörde nicht bei der tatsächlichen Entscheidungsfindung der zuständigen Entscheidungsorganen berücksichtigt.<sup>38</sup> Nachdem HART (im Rahmen eines weitergehenden „Randomised Trials“) in den laufenden Betrieb eingebaut wurde, zeigten sich aber weitere Probleme des zugrunde liegenden Algorithmus, die zu verzerrten Ergebnissen führten.<sup>39</sup> Unter den 34 Kategorien, zu denen Daten der U-Häftlinge erhoben wurden, fand sich auch die Angabe der Postleitzahl des letzten Wohnortes und erhärtete sich der Verdacht, dass die Verwendung solcher geographischer Angaben, die Analyse-Ergebnisse auf unfaire Weise zu Ungunsten von sozio-ökonomisch schwächeren Regionen in Durham beeinflussen könnten; Betroffene aus diesen Regionen also vom HART-System eher als „gefährlich“ eingeschätzt und dementsprechend seltener als für ein Rehabilitationsprogramm geeignet eingestuft würden.<sup>40</sup>

Neben KI-Systemen, die anhand einer Risikoanalyse der „Gefährder“-Früherkennung dient, gibt es weitere Instrumente, die mittels künstlicher Intelligenz versuchen, die Polizeiarbeit zu erleichtern und die verfügbaren Ressourcen besser zu bündeln. Das sogenannte „Predictive Policing“ dient als Überbegriff für eine Vielzahl von Analysetools und – praktiken, die von Polizeibehörden eingesetzt werden, um möglichst akkurat vorherzusehen, wo und wann die nächste Straftat bzw. Reihe von Straftaten begangen werden wird.<sup>41</sup> Die KI-gestützte Analyse wird dabei mit einem fokussierten Ressourceneinsatz, z.B. der Entsendung von Exekutivbeamten zu einem spezifischen Ziel-Areal zu einer gewissen Zeit verbunden. „Predictive Policing“ beinhaltet daher zusätzlich zur Prognose von zukünftigen Straftaten bzw. zur Identifizierung zukünftiger „Kriminalitäts-Hotspots“, meist auch einen verstärkt proaktiven Zugang der Polizeibehörden zur Verbrechensbekämpfung, die auch auf die

---

<sup>33</sup> CENTRE FOR PUBLIC IMPACT, Durham Constabulary's AI decision aid for custody officers (2018), S. 3.

<sup>34</sup> OSWALD/GRACE u.a., Algorithmic risk assessment policing models, in: Information & Communications Technology Law 27:2 (2018), S. 227.

<sup>35</sup> BARANIUK, Durham Police AI to help with custody decisions, BBC (Online), 10.05.2017 (<https://www.bbc.com/news/technology-39857645>; Zugriff am 05.04.2020).

<sup>36</sup> Das Ziel dabei war jedoch nicht, vorherzusagen, wer länger in Haft behalten werden sollte, sondern jene Häftlinge vorzuschlagen, die für ein Rehabilitationsprogramm ausgewählt werden sollten (vgl. CENTRE FOR PUBLIC IMPACT, Durham Constabulary's AI decision aid for custody officers (2018), S. 2-3; sowie BURGESS, UK police are using AI to inform custodial decisions – but it could be discriminating against the poor, in: Wired Magazine (Online), 01.03.2018 (<https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit>; Zugriff am 05.04.2020).

<sup>37</sup> BARANIUK, Durham Police AI to help with custody decisions, BBC (Online), 10.05.2017 (<https://www.bbc.com/news/technology-39857645>; Zugriff am 05.04.2020).

<sup>38</sup> Ebenda.

<sup>39</sup> BURGESS, UK police are using AI to inform custodial decisions – but it could be discriminating against the poor, in: Wired Magazine (Online), 01.03.2018, (<https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit>; Zugriff am 05.04.2020).

<sup>40</sup> OSWALD/GRACE u.a., Algorithmic risk assessment policing models, in: Information & Communications Technology Law 27:2 (2018), S. 228.

<sup>41</sup> BENNETT MOSES/CHAN, Algorithmic prediction in policing, in: Policing and Society 28:7 (2018), S. 807f; mwN.

Identifizierung von optimalen Präventionsmaßnahmen und die laufende Evaluierung der bestehenden Kriminalitätsbekämpfungsstrategien setzt.<sup>42</sup>

Wie sich bereits an der HART-Programm zeigte, kämpft der Einsatz von künstlicher Intelligenz noch mit einigen Problemen. Eine große Herausforderung stellt dabei gerade im Zusammenhang mit KI-unterstützter Prognoseinstrumenten, das Auftreten von Diskriminierungstendenzen dar,<sup>43</sup> die aufgrund von oft intransparenten Vorgängen nicht hinreichend überprüf- und somit nur schwer korrigierbar sind. KI-Systeme sind anfällig dafür, zu „lernen“, voreingenommene Ergebnisse zu liefern und Personen aufgrund irgendeines Parameters oder einer bestimmten Verbindung dieser Parameter zu diskriminieren, ohne dass dies bei der Programmierung jemals intendiert wurde. Ein auf Algorithmen-basierendes System, das rein den Lehren der Logik folgt, mag oberflächlich betrachtet maximal rationale und unvoreingenommene Ergebnisse erwarten lassen, doch ist dies ein Irrtum.<sup>44</sup> Diskriminierende Tendenzen sind häufig bereits ursprünglich angelegt, indem schon bei der Programmierung, diskriminierende Strukturen, die in der „analogen“ Welt bestehen - bewusst oder unbewusst -, im KI-System repliziert werden und sich so auch bei Verwendung dieser neuen Technologien perpetuieren.<sup>45</sup> Dies zeigt eine große Schwäche der KI-Systeme auf, so sie punktuell zwar hervorragende Resultate liefern können, sind sie im Gegensatz zum Menschen nicht in der Lage, komplexe Analysen auszuführen und ist ihre „kognitive“ Flexibilität (noch) stark begrenzt.<sup>46</sup>

Diskriminierende Resultate sind aber bei Weitem nicht das einzige Problemfeld, dass sich beim Einsatz von KI-Systemen im Rahmen von Risikoprognosen ergibt,<sup>47</sup> so stellt etwa die Auswahl und Verfügbarkeit von Datenmaterial eine große Herausforderung dar; der zugrundeliegende Algorithmus kann eben nur auf das eingespeiste Datenmaterial zugreifen, welches oft lokal begrenzt ist und kann diese Limitierung zu gravierenden Fehleinschätzungen führen.<sup>48</sup> Dies muss wohl - zumindest derzeit - zu dem Schluss führen, dass der Einsatz von KI möglichst nur unterstützend herangezogen werden sollte und laufend von menschlichen Anwendern beobachtet und evaluiert werden müssen, um eine „sichere“ Anwendung überhaupt gewährleisten zu können.<sup>49</sup> Zudem wird es unabdingbar sein, dass der zukünftige Anwender sehr genau über die Fähigkeiten und Limitierungen künstlicher Intelligenz in Kenntnis ist und dementsprechend Fehlentwicklungen und falsche Resultate schneller und besser identifizieren kann.<sup>50</sup>

### 2.3. Einsatz künstlicher Intelligenz zur Verbrechensbekämpfung

Wie bereits besprochen, bieten moderne KI-Technologien eine zunehmend attraktive Möglichkeit, personalintensive Aufgaben der Strafverfolgungsbehörden zumindest teilweise durch KI-gestützte Maschinen erfüllen zu lassen und so Kosten und Personal zu sparen. Der Einsatz von künstlicher Intelligenz hat aber auch aus anderen Gründen großes Einsatzpotenzial in diesem Bereich; denn mit zunehmender Digitalisierung ändern

---

<sup>42</sup> BENNETT MOSES/CHAN, Algorithmic prediction in policing, in: Policing and Society 28:7 (2018), S. 806; mwN.

<sup>43</sup> Für die (unbeabsichtigte) Verstärkung von bestehenden Diskriminierungstendenzen durch die Anwendung von KI-Systemen in der Strafverfolgung lassen sich noch einige weitere Beispiele, insbesondere aus dem US-Amerikanischen Raum, wo diese Technologien bereits viel stärker im Strafrechtsbereich eingesetzt werden -, anführen, deren genauere Besprechung würde aber den hier bestehenden Rahmen sprengen; vgl. dazu Vgl. SKEEM/LOWENKAMP, Risk, Race, and Recidivism, in: Criminology 54:4 (2016), S. 680-712.; sowie ANGWIN/ LARSON ua., Machine Bias, ProPublica (Online), 23.05.2016 (<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; Zugriff am 07.04.2020); siehe etwa auch: GUNTER, Chicago goes high-tech in search of answers to gun crime surge, BBC (Online), 19.06.2017, (<https://www.bbc.com/news/world-us-canada-40293666>; Zugriff am 07.04.2020).

<sup>44</sup> ZUIDERVEEN BORGESIJUS, Strengthening legal protection against discrimination by algorithms and artificial intelligence, in: The International Journal of Human Rights (2020), S. 1.

<sup>45</sup> OSWALD/GRACE u.a., Algorithmic risk assessment policing models, in: Information & Communications Technology Law 27:2 (2018), S. 228.

<sup>46</sup> Vgl. TOLAN/MIRON u.a., Why Machine Learning May Lead to Unfairness, in: Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law (ICAIL) (2019), S. 83-92; nachfolgend werden weitere Beispiele dieser Tendenzen näher beleuchtet.

<sup>47</sup> Ein weiteres Problem, kann etwa auch die Ablehnung seitens der intendierten Anwender ein Problem für den effektiven Einsatz von KI-Systemen darstellen, wenn sich diese neuartigen Technologien nicht erfolgreich in die Organisationskultur integrieren lassen (vgl. RATCLIFFE, Jerry/ TAYLOR, Ralph/ FISHER, Ryan, Conflicts and congruencies between predictive policing and the patrol officer's craft, Policing and Society (2019)).

<sup>48</sup> Auch das HART-Programm leidet an einer solchen Einschränkung und verfügt über keinen Zugriff auf landesweite Strafregister, vgl. dazu OSWALD/GRACE u.a., Algorithmic risk assessment policing models, in: Information & Communications Technology Law 27:2 (2018), S. 230; Vgl. auch für den US-Amerikanischen Raum: ANGWIN/LARSON ua., Machine Bias, ProPublica (Online), 23.05.2016 (<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; Zugriff am 07.04.2020).

<sup>49</sup> Ob eine für den österreichischen Standard „sichere“ Anwendung überhaupt möglich ist und wenn ja, in welchen Bereichen, wird erst die weitergehende Analyse im Rahmen der geplanten Dissertation zeigen.

<sup>50</sup> Vgl. BENNETT MOSES/CHAN, Doing Criminological Research on Big Data, Analytics and Predictive Policing, in: Doing Criminological Research, Sage (2018), S. 265 (16); sowie BRAHAN/LAM u.a., AICAMS: artificial intelligence crime analysis and management system, in: Knowledge-Based Systems 11 (1998), S. 361.

sich einerseits die Anforderungen an die Strafverfolgungsbehörden, indem sie mit völlig neuen Formen der Kriminalität konfrontiert sind<sup>51</sup> und eröffnen sich durch die riesigen Datenmengen, die wir inzwischen alle tagtäglich erzeugen, andererseits auch vollkommen neue Quellen zur Sammlung von Beweismaterial.<sup>52</sup> Die riesigen Datenberge stellen eine wahre Goldgrube für die Ermittlungsbehörden dar, sind aber auch eine Herausforderung.<sup>53</sup> Aus dem Umstand allein, riesige Mengen an Daten und somit potentielleres Beweismaterial zur Verfügung zu haben, ist ja an sich noch nichts gewonnen; sondern sind auch entsprechende Instrumente erforderlich, die in Lage sind, dieses Material auch zu analysieren.<sup>54</sup>

Gerade in diesem Bereich der „Big Data“ zeigt sich eines der größten „Talente“ der KI, nämlich die Fähigkeit computationsintensive Aufgaben zu lösen, riesige Datenmengen zu filtern und aufgrund ihrer überragenden Rechenleistung analytische Spitzenresultate zu erzielen, zu welchen der menschliche Geist niemals in der Lage wäre („Data Mining“).<sup>55</sup> Ein Gebiet, das sich daher hervorragend für den Einsatz künstlicher Intelligenz eignet, ist die Bild-Analyse, die beispielsweise zur Bekämpfung der Verbreitung von kinderpornographischem Bilder- und Videomaterial im Internet zum Einsatz kommt und dabei vielversprechende Resultate zeigt.<sup>56</sup> Maschinen lernen dabei etwa textile Strukturen im Hintergrund kinderpornographischen Materials zu identifizieren und mit bereits bekannten Struktursets zu matchen. Während das menschliche Auge mit der Flut an visuellen Informationen aus Abermillionen Bild- und Videodateien vollkommen überfordert ist, kann ein KI-System, Unmengen an Datenmaterial blitzschnell sichten, Datensets erstellen und Verbindungen zwischen einzelnen Dateien herstellen, die sonst wahrscheinlich unentdeckt geblieben wären. Derart können dann zB. mehrere Bilder bzw. Videos, die dieselben Vorhänge oder dieselbe Bettwäsche zeigen, zu einem Daten-Set verbunden und so in Folge einem individuellen „Hersteller“ zugeordnet werden.<sup>57</sup> Die sich so ergebenden Sets, erlauben dann eine tiefere Analyse und decken möglicherweise weitere Details auf, welche sich zu einer konkreten Spur zum Täter, Tatort oder zum Opfer verdichten können.

Neben diesem Einsatz in der Bildanalyse finden KI-unterstützte Technologien etwa in der bereits angesprochenen Überwachung bzw. Sichtung von Geldwäsche-verdächtigen Bank-Transaktionen<sup>58</sup> oder der Aufdeckung von Strukturen organisierter Kriminalität Anwendung.<sup>59</sup> Ein weiteres interessantes Einsatzfeld findet sich z.B. bei polizeilichen Einvernahmen, wo Noriega argumentiert, dass KI-unterstützte Systeme, dazu beitragen können, unzulässige Voreingenommenheit und Vorurteilen (zB rassistischer oder sexistischer Natur) vorzubeugen und das Risiko falscher Geständnisse zu verringern.<sup>60</sup> Zudem finden sich Beispiele von KI-Anwendungen auf internationaler Ebene bereits in vielen weiteren Bereichen insbesondere des Ermittlungsverfahrens, wobei eine nähere Darstellung aufgrund des begrenzten Rahmens hier unterbleiben muss.<sup>61</sup>

### 3. Forschungsfragen

Diese Dissertation zielt darauf ab, die derzeitigen und zukünftigen Anwendungsbereiche künstlicher Intelligenz im Bereich der Strafverfolgung zu untersuchen und soll hierbei jeweils die nationale, europäische als auch internationale Ebene beleuchtet werden. Der Fokus wird dabei neben der nationalen Ebene voraussichtlich vor

---

<sup>51</sup> KING/AGGARWAL u.a., Artificial Intelligence Crime, in: Science and Engineering Ethics 26 (2020), S. 90.

<sup>52</sup> BENNETT MOSES/CHAN, Doing Criminological Research on Big Data, Analytics and Predictive Policing, in: Doing Criminological Research, Sage (2018), S. 265 (16).

<sup>53</sup> BOWCOTT/DEVILIN, Police trial AI software to help process mobile phone evidence, in: the Guardian (Online), 27.05.2018 (<https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence>; Zugriff am 05.04.2020).

<sup>54</sup> Vgl. etwa das „DARPA Memex Program“, dazu: SZEKELY/KEJRIWAL, Domain-specific Insight Graphs (DIG), in: WWW '18 Companion: The 2018 Web Conference Companion (2018), S. 433-434.

<sup>55</sup> DUAN/EDWARDS/DWIVEDI, Artificial intelligence for decision making in the era of Big Data, in: International Journal of Information Management 48 (2019), S. 69; sowie dazu weiter NISSAN, An Overview of Data Mining for Combating Crime, Applied Artificial Intelligence, 26:8 (2012), S. 760-786. Zu den Grundlagen siehe auch vgl. CHEN/SHIWEN/YUNHAO, Big data, in: Mobile networks and applications 19:2 (2014), S. 171-209).

<sup>56</sup> BARANIUK, The new weapon in the fight against crime, in: BBC Future (Online), 04.03.2019 (<https://www.bbc.com/future/article/20190228-how-ai-is-helping-to-fight-crime>; Zugriff am 04.04.2020).

<sup>57</sup> GARCÍA-OLALLA/ALEGRE u.a., Textile Retrieval Based on Image Content from CDC and Webcam Cameras in Indoor Environments, in: Sensors 18 (2018).

<sup>58</sup> WATKINS/REYNOLDS u.a., Tracking dirty proceeds, in: Police Practice and Research, 4:2 (2003), S. 163-178.

<sup>59</sup> NISSAN, Legal evidence and advanced computing techniques for combatting crime, in: Information & Communications Technology Law, 22:3 (2013), S. 234f.

<sup>60</sup> NORIEGA, The application of artificial intelligence in police interrogation, in: Futures 117 (2020).

<sup>61</sup> Für einen weiteren Überblick etwa NISSAN, Legal evidence and advanced computing techniques for combatting crime, in: Information & Communications Technology Law, 22:3 (2013), S. 213-250.

allem auf den anglo-amerikanischen und den EU-Raum gerichtet werden; ein Ausblick auch auf den ost-asiatische Raum, insbesondere auf China, könnte ebenfalls interessante Erkenntnisse bringen. Nach eingehender Untersuchung der Anwendungsbereiche selbst, sollen die mit dem Einsatz von künstlicher Intelligenz verbundenen Chancen und Herausforderungen tiefgehend analysiert werden und diese sodann auch in Bezug zur österreichischen Rechtsordnung gesetzt und beleuchtet werden, inwieweit und unter welchen Voraussetzungen die Verwendung von KI-Systemen in der österreichischen Strafverfolgung Raum hat und welche Veränderungen für einen Einsatz solcher Technologien unter Umständen nötig wären. Bei dieser Bearbeitung sollen aber nicht nur die rechtlichen Problemstellungen, die sich aus der Anwendung (oder aber auch der Nichtanwendung) von KI in der Strafverfolgung ergeben, erörtert werden, sondern soll möglichst auch eine weitergehende Diskussion darüber, welche Folgen die Adaption von KI auf gesellschaftlicher Ebene haben kann, zumindest mitangestoßen werden.<sup>62</sup> Zum Abschluss der Arbeit, sollen Lösungsansätze dargestellt werden, mit welchen man den Problemen zu begegnen versucht, die sich derzeit beim Einsatz von KI in diesem Bereich ergeben. Zum Abschluss soll auch ein kurzer Ausblick gegeben werden, darüber, mit welchen Entwicklungen im Bereich künstlicher Intelligenz bezogen auf das untersuchte Einsatzfeld „Strafverfolgung“ auf kurzer, mittelfristiger und langer Sicht zu rechnen ist. Die Forschungsfragen lassen sich daher wie folgt zusammenfassen:

- Wie können KI-Systeme als Instrument der Strafverfolgung im Rahmen der Verbrechensprävention eingesetzt werden und welche Anwendungsbeispiele lassen sich finden?
- Wie können KI-Systeme als Instrument der Strafverfolgung im Rahmen der Verbrechensbekämpfung eingesetzt werden und welche Anwendungsbeispiele lassen sich finden?
- Gibt es auf nationaler Ebene bereits Anwendungsbereiche und welche Unterschiede ergeben sich dabei, im Vergleich zur Anwendung auf internationaler Ebene (insb. US, UK, EU)?
- Bestehen hinreichende Rahmenbedingungen für den Einsatz von KI-Systemen im nationalen Rechtssystem?
- Welche Probleme ergeben sich durch den Einsatz von KI-Systemen und welche Lösungsansätze bestehen für diese?
- Welche Entwicklungen sind auf diesem Gebiet im Bereich Strafverfolgung zu erwarten?

Anzumerken ist hier noch, dass bereits die vorläufigen Recherche gezeigt hat, dass es teilweise erhebliche Abweichungen bei der Verwendung grundlegender Begrifflichkeiten (angefangen schon beim Begriff „Künstliche Intelligenz“ selbst) gibt und die vornehmlich aus dem anglo-amerikanischen Raum stammenden Literatur, auf ein vom österreichischen System abweichendes Rechtssystem ausgelegt ist; es wird jedenfalls durchgängig von großer Bedeutung sein, Begriffe klar zu definieren und einheitlich zu verwenden und Abgrenzungen etwa zwischen den Einsatzbereichen "Verbrechensprävention" und „Verbrechensbekämpfung“ möglichst klar zu ziehen.

#### 4. Forschungsmethoden

Diese Arbeit wird vor allem auf die einschlägige wissenschaftliche Literatur in diesem Bereich zurückgreifen und zur Vervollständigung auch Berichte, White Papers und Guidelines relevanter Behörden und Organisationen, sowie Medienberichte heranziehen. Weiters soll auch einschlägige Rechtsprechung auf nationaler, europäischer und internationaler Ebene untersucht werden, so sich diese auffinden lässt; wo diese fehlt, wird geprüft werden, ob sich anhand der bestehenden Rechtsprechung zu ähnlich gelagerten Problemstellungen stichhaltige Ableitungen für die hier relevanten Fragen treffen lassen. Auch soll mittels juristischer Interpretationsmethoden untersucht werden, ob die bestehenden Bestimmungen des Polizei-, Straf- und Strafprozessrechts bereits jetzt hinreichende Rahmenbedingungen für den Einsatz von KI-Systemen bieten und eine Einbindung in die Strafverfolgung rechtstaatlich gedeckt wäre bzw. welche Schritte notwendig wären, um eine solche Einbindung zu gewährleisten.

So sich diese als erforderlich erweisen (mangels verwertbaren oder zugänglichen Materials u.ä.), wären auch Interviews mit Wissenschaftlern in den relevanten Bereichen angedacht; dies könnte nötig werden, um

---

<sup>62</sup> Vgl. CRAWFORD/DOBBE u.a., AI Now 2019 Report, AI Now Institute (2019), S. 6f.



insbesondere den technischen Hintergrund hinreichend zu durchdringen und nachvollziehbarer darlegen zu können, sowie aktuelle Entwicklungen auf diesem Gebiet besser identifizieren zu können.

Auch Interviews mit Entscheidungsträgern bzw. Organen der Strafverfolgungsbehörden werden überlegt und könnten diese wichtigen Einblicke in die praktische Anwendung und Anwendbarkeit dieser neuen Technologien liefern und helfen, konkrete Problemstellungen, die sich beim Einsatz in der Praxis ergeben, zu erhellen. Die Undurchführbarkeit derartiger Interviews aufgrund fehlender Gesprächsbereitschaft seitens der Behörden ist dabei aber jedenfalls einzukalkulieren.

## 5. Aktueller Forschungsstand

Bei Durchsicht der bestehenden Literatur zum Forschungsgegenstand fällt auf, dass vor allem aus dem anglo-amerikanischen Raum einschlägige Literatur vorliegt, was wohl auch auf den dortig weitverbreiteten Einsatz von KI-Systemen in der Strafverfolgung zurückzuführen ist. Die bestehende Literatur bildet klar ab, dass es sich bei künstlicher Intelligenz um ein neues und rasant wachsendes Phänomen handelt und deren Einsatz und Weiterentwicklung im Strafverfolgungsbereich eine Vielzahl von fundamentalen Fragen aufwirft, zu denen häufig noch tiefgreifendere Untersuchungen fehlen. In der bisherigen wissenschaftlichen Aufarbeitung wird etwa auf Probleme mit der Untersuchung dieser Technologien und ihrer Anwendung im Strafverfolgungsbereich hingewiesen. Es stellt sich zB die Frage, wie man zu wissenschaftlich fundierten Erkenntnissen gelangen kann, wenn typische Instrumente der Wissenschaft, wie etwa ein „Double Blind Trial“ aus ethischen und rechtlichen Gründen überhaupt nicht zur Verfügung steht; so etwa der Fall bei der Wirksamkeitsüberprüfung von KI-Systemen bei der Gefährder-Risikoanalyse, wo es ethisch und rechtlich niemals vertretbar wäre, wissentlich eine als „Hochrisiko“ eingestufte Person aus der Haft zu entlassen, nur um die Treffsicherheit eines Algorithmus zu testen.<sup>63</sup> Insgesamt wird seitens der bestehenden Literatur auch aufgezeigt, dass es noch erheblich an Verständnis mangelt, was den Einsatz von KI und ihre häufig sehr komplexen Funktionsmechanismen betrifft und stellt sich letztendlich oft auch die Frage, ob die Ergebnisse von KI-gestützten Anwendungen überhaupt die rechtlichen Anforderungen, die im Rahmen eines strafrechtlichen Verfahrens zu erfüllen sind, befriedigen können (z.B. Beweisqualität, Nachvollziehbarkeit von Prognosen, Legalität von Ermittlungsmaßnahmen, etc.); und auch ob und wie es möglich sein wird, den Einsatz dieser Technologien mit dem bestehenden System von Grund- und Menschenrechte zu vereinbaren.

Der Einsatz von KI in den hier zu beleuchtenden Bereichen, berührt neben diversen Verteidigungsrechten, wie dem Recht auf ein faires Verfahren (Art 6 EMRK), weitere sensible Grundrechte wie das Recht auf Privatleben und Privatsphäre (Art 8 EMRK), das Grundrecht auf Datenschutz<sup>64,65</sup> und hat potenzielle Auswirkungen auch auf Grundfreiheiten wie das Versammlungsrecht, die Glaubens- und Meinungsfreiheit und auch auf die Menschenwürde selbst (Art 1 GRC). Dies alles sind Rechte, die letztendlich das Fundament unseres bestehenden demokratischen und rechtsstaatlichen Systems absichern. Es stellt sich auch die Frage, ob KI unterstützte Technologien in der staatlichen Strafverfolgung die strengen Anforderungen hinsichtlich Verhältnismäßigkeit und Notwendigkeit ihres Einsatzes erfüllen. Neben der Prüfung dieser Aspekte wird aber etwa auch die Haftung für Fehler beim Einsatz dieser Technologien noch zu klären sein.<sup>66,67</sup> Aufgrund der erheblichen Sensibilität des Einsatzbereiches, der mit erheblichen Eingriffen in Grund- bzw. Menschenrechte verbunden ist, kommt einer zeitnahen wissenschaftlichen Aufarbeitung dieses Themenkomplexes daher jedenfalls ein hoher Stellenwert zu.

## 6. Vorläufige Gliederung

### I. Einleitung

- I.1. Problemstellung
- I.2. Methodenwahl

---

<sup>63</sup> OSWALD/GRACE u.a., Algorithmic risk assessment policing models, in: Information & Communications Technology Law 27:2 (2018), S. 226

<sup>64</sup> Wobei dieser „Datenschutz“-Begriff weit zu verstehen ist und auch den Schutz der Persönlichkeit bzw. der Persönlichkeitsrechte und dabei insbesondere des Rechts „auf informationelle Selbstbestimmung“ gemeint ist, vgl. dazu HILGENDORF, Digitalisierung, Virtualisierung und das Recht, in: Künstliche Intelligenz - Fluch oder Segen, (2020), S. 53-54.

<sup>65</sup> JOHNSON/NAPIERLSKI/ŠKORJANC, INTERPOL World 2019 und 2nd INTERPOL-UNICRI Global Meeting on Artificial Intelligence for Law Enforcement, in: Künstliche Intelligenz - Fluch oder Segen, (2020), S. 110.

<sup>66</sup> OSWALD/GRACE u.a., Algorithmic risk assessment policing models, in: Information & Communications Technology Law 27:2 (2018), S. 230.

<sup>67</sup> Vgl. BURTON/HABLI u.a., Mind the gaps, in: Artificial Intelligence 279 (2020).

- I.3. Forschungsziel
- II. Was ist künstliche Intelligenz?**
  - II.1. Entwicklung und Übersicht
  - II.2. Künstliche Intelligenz und Recht
- III. Nutzung künstlicher Intelligenz in der Verbrechensprävention**
  - III.1. Entwicklung
  - III.2. „Predictive Policing“
  - III.3. Facial and Voice Recognition und Analyse molekulargenetischen Materials (Biometrics)
  - III.4. „Offender Risk-Analysis“
  - III.5. Übersicht aktueller Einsatzarten in internationaler Zusammenschau
- IV. Nutzung künstlicher Intelligenz in der Verbrechensbekämpfung**
  - IV.1. Entwicklung
  - IV.2. KI-gestützte Ermittlungsmaßnahmen
  - IV.3. Videoanalyse und Datamining
  - IV.4. Facial and Speech Recognition und Analyse molekulargenetischen Materials
  - IV.5. Übersicht aktueller Einsatzarten in internationaler Zusammenschau
- V. Problemfelder**
  - V.1. Menschen- und Grundrechtliche Absicherung
    - V.1.1. Recht auf Datenschutz, Recht auf Schutz des Privatlebens
    - V.1.2. Schutz der Menschenwürde, Recht auf Freiheit und Sicherheit, Recht auf freie Meinungsäußerung, Recht auf Versammlungsfreiheit, „chill effect“
    - V.1.3. Recht auf ein faires Verfahren, Verteidigungsrechte, Rechtliches Gehör, Verbot automatisierter Entscheidungen, Verhältnismäßigkeit, Rechtsmittel
    - V.1.4. Recht auf eine gute Verwaltung
  - V.2. Sorgfaltsanforderungen
    - V.2.1. Verlässlichkeit der Technik und Gewährleistung angemessener Input-Qualität
    - V.2.2. Transparenz und laufende Überprüfung
    - V.2.3. „Human-in-the-loop“, „Human-on-the-loop“, menschliche Supervision
    - V.2.4. „privacy by design“?
  - V.3. Haftung
    - V.3.1. Nachvollziehbarkeit und Zurechenbarkeit
    - V.3.2. Zugang zu Rechtsschutz
- VI. Prognose und Schlussfolgerungen**

## 7. Zeitplan

April - September 2020: Erstellung des Exposé

Oktober 2020: Fakultätsöffentliche Präsentation des Dissertationsvorhabens

Jänner 2021: Einreichung Exposé und Antrag auf Genehmigung des Dissertationsvorhabens

Juli 2020 – Oktober 2020: Verfassen der Kapitel 1-2

Oktober 2020 – Jänner 2021: Verfassen der Kapitel 3-5

Februar 2021 – April 2021: Verfassen der Kapitel 6

Mai 2021 – Juli 2021: Kontrolle und Überarbeitung der Dissertation

August 2021: Abgabe an Betreuer

Oktober 2021: öffentliche Defensio

## 8. Vorläufige Literatur

**ALZOU, Suhaib/ ALZOU, Bi/ ALSHIBLY, Haitham/ AL-MA'AITAH, Mohammad**, Artificial Intelligence in Law Enforcement, A Review, in: International Journal of Advanced Information Technology 4 (2014).

**ANGWIN, Julia/ LARSON, Jeff/ MATTU, Surya/ KIRCHNER, Lauren**, Machine Bias, There's software used across the country to predict future criminals. And it's biased against blacks, ProPublica (Online), 23.05.2016 (<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; 07.04.2020).

**BARANIUK, Chris**, Durham Police AI to help with custody decisions, BBC (Online), 10.05.2017 (<https://www.bbc.com/news/technology-39857645>; Zugriff am 05.04.2020).

**BARANIUK, Chris**, The new weapon in the fight against crime, in: BBC Future (Online), 04.03.2019 (<https://www.bbc.com/future/article/20190228-how-ai-is-helping-to-fight-crime>; Zugriff am 04.04.2020).

**BENNETT MOSES, Lyria/ CHAN, Janet**, Algorithmic prediction in policing: assumptions, evaluation, and accountability, in: Policing and Society 28:7 (2018), S. 806-822.

**BENNETT MOSES, Lyria/ CHAN, Janet**, Doing Criminological Research on Big Data, Analytics and Predictive Policing, in: DAVIES Pamela/ FRANCIS, Peter [Hrsg.]: Doing Criminological Research<sup>3</sup>, Sage Publications Ltd (2018), S. 251-270.

**BOWCOTT, Owen/ DEVLIN, Hannah**, Police trial AI software to help process mobile phone evidence, in: the Guardian (Online), 27.05.2018 (<https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence>; Zugriff am 05.04.2020).

**BRAHAN, John/ LAM, Kai/ CHAN, Hilton/ LEUNG, William**, AICAMS: artificial intelligence crime analysis and management system, in: Knowledge-Based Systems 11 (1998), S. 355–361.

**BURGESS, Matt**, UK police are using AI to inform custodial decisions – but it could be discriminating against the poor, in: Wired Magazine (Online), 01.03.2018, (<https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit>; Zugriff am 05.04.2020).

**BURTON, Simon/ HABLI, Ibrahim/ LAWTON, Tom/ MCDERMID, John/ MORGAN, Phillip/ PORTER, Zoe**, Mind the gaps: Assuring the safety of autonomous systems from an engineering, ethical, and legal perspective, in: Artificial Intelligence 279 (2020).

**CAMPELL, Charlie**, The Entire System Is Designed to Suppress Us. What the Chinese Surveillance State Means for the Rest of the World, in: Time Magazine (Online), 21.11.2019 (<https://time.com/5735411/china-surveillance-privacy-issues/>; Zugriff am 24.05.2020).

**CENTRE FOR PUBLIC IMPACT**, Durham Constabulary's AI decision aid for custody officers, A case study on the use of AI in government (2018).

**CHEN, Min/ SHIWEN, Mao/ YUNHAO, Liu**, Big data: A survey, in: Mobile networks and applications 19:2 (2014), S. 171-209.

**CRAWFORD, Kate/ DOBBE, Roel u.a.**, AI Now 2019 Report, AI Now Institute, New York University (2019).

**DELOITTE**, The case for artificial intelligence in combating money laundering and terrorist financing, Deloitte white paper (2018), (<https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/finance/sea-fas-deloitte-uob-whitepaper-digital.pdf>; Zugriff am 07.04.2020).

**DJEFFAL, Christian**, Normative Leitlinien für künstliche Intelligenz in Regierung und öffentlicher Verwaltung, in: MOHABBAT KAR/ THAPA/ PARYCEK [Hrsg.]: (Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft (2018), S. 493-515.

**DUAN, Yanqing/ EDWARDS, John/ DWIVEDI, Yogesh**, Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research, in: International Journal of Information Management 48 (2019), S. 63-71.

**DWIVEDI, Yogesh/ HUGHES, Laurie/ ISMAGILOVA, Elvira/ AARTS, Gert** u.a., Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, in: International Journal of Information Management (2019) (in press).

**FELDSTEIN, Steven**, The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, 17.09.2019 (<https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>); Zugriff am 24.05.2020).

**GARCÍA-OLALLA, Oscar/ ALEGRE, Enrique/ FERNÁNDEZ-ROBLES, Laura/ FIDALGO, Eduardo/ SAIKIA, Surajit**, Textile Retrieval Based on Image Content from CDC and Webcam Cameras in Indoor Environments, in: Sensors 18 (2018).

**GUNTER, Joel**, Chicago goes high-tech in search of answers to gun crime surge, BBC (Online), 19.06.2017, (<https://www.bbc.com/news/world-us-canada-40293666>); Zugriff am 07.04.2020).

**HILGENDORF, Eric**, Digitalisierung, Virtualisierung und das Recht, in: REINDL-KRAUSKOPF, Susanne/ GRAFL, Christian [Hsgb]: Künstliche Intelligenz - Fluch oder Segen, (2020), S. 37 -58.

**HUANG, Shigao/ YANG, Jie/ FONG, Simon/ ZHAO, Qi**, Artificial intelligence in cancer diagnosis and prognosis: Opportunities and challenges, in Cancer Letters 471 (2020), S. 61–71.

**INTERNATIONAL DATA CORPORATION (IDC)**: Automation and Customer Experience Needs Will Drive AI Investment to \$5 Billion by 2019 Across European Industries, 2019 (<https://www.idc.com/getdoc.jsp?containerId=prEMEA44978619>); Zugriff am 09.04.2020).

**JOHNSON, Emily/ NAPIERALSKI, Antoni/ ŠKORJANC, Žiga**, INTERPOL World 2019 und 2nd INTERPOL-UNICRI Global Meeting on Artificial Intelligence for Law Enforcement, in REINDL-KRAUSKOPF, Susanne/ GRAFL, Christian [Hsgb]: Künstliche Intelligenz - Fluch oder Segen, (2020), S. 101-117.

**KAPLAN, Andreas/ HAENLEIN, Michael**, Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence, in: Business Horizons 62:1 (2019), S. 15-25.

**KINGDON, Jason**, AI Fights Money Laundering, the IEEE Computer Society (2004) (<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1315546>); Zugriff am 07.04.2020).

**KOUZIOKAS, Georgios**, The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment, in: Transportation Research Procedia 24 (2017) S. 467–473.

**MÜLLER, Vincent/ BOSTROM Nick**, Future Progress in Artificial Intelligence: A Poll among Experts, in: AI Matters 1:1 (2014), S. 9-11.

**NISSAN, Ephraim**, Legal evidence and advanced computing techniques for combatting crime: an overview, in: Information & Communications Technology Law, 22:3 (2013), S. 213-250.

**NISSAN, Ephraim**, An Overview of Data Mining for Combating Crime, Applied Artificial Intelligence, 26:8 (2012), S. 760-786.

**NORIEGA, Maria**, The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions, in: Futures 117 (2020).

**NUNN Samuel**, When Superman Used X-Ray Vision, Did He Have a Search Warrant? Emerging Law Enforcement Technologies and the Transformation of Urban Space, in: Journal of Urban Technology, 9:3 (2002), S. 69-87.

**OSWALD, Marion/ GRACE, Jamie/ URWIN, Sheena/ BARNES, Geoffrey**, Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, in: Information & Communications Technology Law 27:2 (2018), S. 223-250

**PAPPAS, Ilias/ MIKALEF, Patrick/ GIANNAKOS, Michail/ KROGSTIE, John/ LEKAKOS, George**, Big data and business analytics ecosystems: Paving the way towards digital transformation and sustainable societies, in: Information Systems and e-Business Management, 16:3 (2018), S. 479–491.

**RATCLIFFE, Jerry/ TAYLOR, Ralph/ FISHER, Ryan**, Conflicts and congruencies between predictive policing and the patrol officer's craft, *Policing and Society* (2019).

**RUEP, Stefanie**, Schutzzonen für das Menschliche trotz künstlicher Intelligenz, in: *der Standard* (online), 03.02.2020 (<https://www.derstandard.at/story/2000113987689/schutzzonen-fuer-das-menschliche-trotz-kuenstlicher-intelligenz>; Zugriff am 16.05.2020).

**SKEEM, Jennifer/ LOWENKAMP Christopher**, Risk, Race, and Recidivism: Predictive Bias and Disparate Impact, in: *Criminology* 54:4 (2016), S. 680-712.

**SZEKELY, Pedro/ KEJRIWAL, Mayank**, Domain-specific Insight Graphs (DIG), in: *WWW '18 Companion: The 2018 Web Conference Companion* (2018), S. 433-434.

**TOLAN, Songül/ MIRON, Marius/ GOMEZ, Emilia/ CASTILLO, Carlos**, Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia, in: *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law (ICAIL)* (2019), S. 83–92.

**WATKINS, Cory/ REYNOLDS, Michael/ DEMARA, Ron/ GEORGIPOULOS, Michael/ GONZALES, Avelino/ EAGLIN, Ron**, Tracking dirty proceeds: Exploring data mining technologies as tools to investigate money laundering, in: *Police Practice and Research*, 4:2 (2003), S. 163-178.

**ZUIDERVEEN BORGESIU, Frederik**, Strengthening legal protection against discrimination by algorithms and artificial intelligence, in: *The International Journal of Human Rights* (2020).