Kristin Pfeffer (Herausgeber)

SMART BIG DATA POLICING – Chancen, Risiken und regulative Herausforderungen

5. Hamburger Sicherheitsrechtstag

https://cuvillier.de/de/shop/publications/8772

Begrüßung anlässlich des 5. Hamburger Sicherheitsrechtstages an der Akademie der Polizei Hamburg

Mirko Streiber[1]

Sehr geehrte Frau Prof. Dr. Pfeffer,

sehr geehrte Angehörige der Forschungsstelle für Europäisches und Deutsches Sicherheitsrecht,

liebe Gäste hier im großen Sitzungssaal und vor den Bildschirmen,

ich begrüße Sie ganz herzlich zum 5. Hamburger Sicherheitsrechtstag mit dem Themenschwerpunkt SMART BIG DATA POLICING.

Smarte Polizeiarbeit

Der Spagat zwischen Freiheit, Sicherheit und Überwachung.

Die sich mit unglaublicher Geschwindigkeit entwickelnde Digitalisierung, oder präziser ausgedrückt die ***„digitale Transformation der Gesellschaft“,*** beeinflusst auch die Kriminalitätsentwicklung und führt unweigerlich zum Umdenken und Neudenken der polizeilichen Arbeit.

Die digitale Welt erleichtert uns den Alltag – bietet zeitgleich aber auch Kriminellen diverse Möglichkeiten für Missbrauch.

Cyberterrorismus ist eine reale Bedrohung für Staat, Gesellschaft und Wirtschaft. Und so führt uns der aktuelle russische Angriffskrieg unmittelbar vor Augen, wie sensibel und digital abhängig unsere kritische Infrastruktur mittlerweile ist.

Dabei sind nicht nur kritische Bereiche wie Energie, Verkehr, Bankwesen und Gesundheit zu schützen, sondern auch die für die digitale Kommunikation erforderlichen Netze.

[1] Polizeivizepräsident der Polizei Hamburg.

Die Zahl und Komplexität von Cyberangriffen und Cyberkriminalität nimmt in ganz Europa zu. Diese Tendenz dürfte in Zukunft noch steigen, da bis 2024 voraussichtlich 22,3 Milliarden Geräte weltweit mit dem Internet verbunden sein werden.

Terrororganisationen nutzen erfolgreich die Digitalisierung und verbreiten ihre extremistischen Ansichten weltweit in sozialen Netzwerken, um neue Anhänger zu gewinnen.

Auch links- und insbesondere rechtsextremistische Strömungen haben den Nutzen der sozialen Medien erkannt und verbreiten hierüber ihre kruden Ideologien, die gerade in Krisenzeiten auf fruchtbaren Boden fallen.

Hier ist vor allem eine effektive Vernetzung von Polizei, Verfassungsschutz und Nachrichtendiensten erforderlich.

Verbrechen werden durch die Digitalisierung internationaler und die Verarbeitung digitaler Spuren immer bedeutsamer – professionell organisierte Kriminelle nutzen sämtliche Chancen aus, sind gut vernetzt und agieren länderübergreifend.

Die Nachfrage an kriminellen Dienstleistungen im kriminellen Raum des Internets -Stichwort Darknet- wächst, Grauzonen dehnen sich immer weiter aus.

Die Anonymität ermöglicht es, Zugang zu jeder Art von illegalen Geschäften, wie z.B. Drogen- und Waffenhandel, Identitätsdiebstahl bis hin zu Anleitungen zu Sprengstoffattentaten zu erhalten.

Auch nicht profitorientierte, sondern ideologisch motivierte Hackerangriffe schwächen die innere Sicherheit.

Die verstärkte Nutzung von Home-Office und die ständig wachsende Zahl an Online-Shops, bieten auch Allgemeinkriminellen lukrative Betrugsmöglichkeiten.

Kriminalität verlagert sich mehr und mehr ins Netz und die Polizei ist gefordert, hier Schritt zu halten. Täter hinterlassen bei ihren Aktivitäten im digitalen Raum eine Vielzahl von digitalen Spuren, die für die Aufklärung von Straftaten großes Potential bieten, deren Verarbeitung die Ermittlungsbehörden aber vor immense Herausforderungen stellt.

Ein Blick auf die jährliche Kriminalstatistik zeigt, dass die Taten im Bereich der Internetkriminalität kontinuierlich ansteigen. So wies die letzte Kriminalitätsstatistik in Hamburg eine Steigerung von rund 9 % auf.

Sicherlich hat hier die Corona-Pandemie einen wesentlichen Beitrag geleistet.

In Zeiten von Lock-Downs und Home-Office ist die digitale Welt ein treuer und ständiger Begleiter gewesen, sowohl im Berufsleben als auch im privaten Bereich. Auch für diejenigen, die zuvor vielleicht nicht ständig „online“ waren.

Aber die Pandemie war dabei nur ein Booster für die Entwicklung der Kriminalitätsverlagerung in den digitalen Raum. Der Trend zeichnet sich mittlerweile seit Jahren ab.

Der moderne Polizeiansatz „Smart Policing“ beschreibt die Nutzung intelligent vernetzter Objekte und algorithmischer Systeme (Big-Data-Analysen) für die Ausübung polizeilicher Aufgaben.

Tools, die im Rahmen dieses Ansatzes eingesetzt werden, sind beispielsweise Predictive-Policing Lösungen. Dessen Nutzung haben wir als Polizei Hamburg für den Bereich Einbruch geprüft und dabei festgestellt, dass eine rein technische Lösung nicht zielführend ist. Vielmehr bedarf es neben einer Professionalisierung der Lagedarstellung, der Datenqualität und der Geodateninfrastruktur vor allem der menschlichen Komponente für eine professionelle Auswertung und Analyse der Daten.

Die Geburtsstunde des Berufsbildes Kriminalitätsanalytik ist ein gutes Beispiel dafür, dass Technik nicht alles ist, sondern es vielmehr auf die Synergie aus Mensch und Technik ankommt.

Der Begriff „Big Data“ (Massendaten) wiederum steht in engem Zusammenhang mit dem umfassenden Prozess der „Datafizierung“. Datenmengen werden einfach zu groß, zu komplex, zu schnelllebig oder sind zu unstrukturiert, um sie mit manuellen und herkömmlichen Methoden der Datenverarbeitung auszuwerten.

Diese Massendaten können aus verschiedensten Quellen stammen, wie z.B.:

- Aufzeichnungen von Überwachungssystemen
- Kunden-, Bank- bzw. Bezahlkartendaten und deren Nutzung

- jeglicher elektronischen Kommunikation

Oder es handelt sich um Daten aus dem Internet der Dinge, dessen Bedeutung in Zeiten intelligenter Kraftfahrzeuge und Smart Home Technologie stetig wächst.
Klassische relationale Datenbanksysteme sowie Statistik- und Visualisierungsprogramme oder gar manuelle, händische Verarbeitungsmethoden sind kaum oder gar nicht mehr in der Lage, derart große Datenmengen zu verarbeiten.

Für die Verarbeitung von Massendaten sind daher neue Arten von Datenspeicher- und Analyse-Systeme erforderlich.

In der kriminalistischen Fallbearbeitung gewinnt die Verarbeitung von digitalen Spuren und Beweismitteln immer mehr an Bedeutung. Die Sicherung, Aufbereitung und Auswertung digitaler Daten stellen aufgrund der dynamischen Entwicklungen im Bereich der Informations- und Kommunikationstechniken und der damit verbundenen exponentiell zunehmenden Datenmengen eine besondere Herausforderung für uns als Strafverfolgungsbehörden dar.

Der Masse an sichergestellten Daten steht dabei ein Mangel an Ressourcen der Strafverfolgungsbehörden gegenüber. Dies betrifft personelle Ressourcen, ebenso wie die Sachmittelausstattung. Aber machen wir uns nichts vor: Wir können noch so viel Personal und Auswerter einstellen, damit werden wir der Massenflut nicht Herr.

Vielmehr verlieren wir dadurch nicht nur den Kampf gegen die Internetkriminellen, sondern auch die Attraktivität unseres Berufes. Denn die eintönige Arbeit frustriert auf Dauer und lässt sich kaum noch mit dem Bild des ermittelnden Crimefighter vereinbaren.

Ziel muss es deshalb sein, über automatisierte Prozesse eine Selektion, sowie Reduktion von derzeit noch manuell auszuwertenden Daten zu erreichen, um zielgerichtete Analyseansätze zu erhalten. Dies schont nicht nur Ressourcen, sondern generiert Zeitgewinne, die weitere Straftaten verhindern und im Extremfall Leben retten können.

Der Einsatz von Techniken Künstlicher Intelligenz (KI) kann hierbei z.B. in definierten Fällen die Sachbearbeitungen erheblich entlasten. Versuche laufen derzeit bereits beim LKA Niedersachsen in Bezug auf die Verarbeitung von kinderpornografischem Material.

Hamburg steht im engen Kontakt mit Niedersachsen, nutzt aber derzeit noch keine Künstliche Intelligenz. Das LKA 25, die Dienststelle für die Telekommunikationsüberwachung, bedient sich einer anderen Technik zur Auswertung von Massendaten. Mithilfe der vom LKA selbst entwickelten Anwendung URAN -Universelle Rohdatenanalyse- lassen sich im Rahmen einer Telekommunikationsüberwachung neben den reinen Sprachdaten auch die übermittelten unverschlüsselten Metadaten bzw. Begleitdaten der Kommunikation analysieren und auswerten.

Das ist nur ein Beispiel von vielen, da ist noch sehr viel Luft nach oben und die Herausforderung besteht darin, bei der Datenflut die Übersicht zu behalten. Denn wir wissen eigentlich gar nicht, was wir alles wissen!

Das Problem besteht darin, dass wir in vielen unterschiedlichen Datentöpfen Informationen haben, welche wir auch rechtmäßig verarbeiten können und dürfen. Allerdings erkennen wir durch die manuelle Herangehensweise die Zusammenhänge erst spät oder vielleicht gar nicht.

Einem Ermittler ist es heute in Hamburg z.B. nicht möglich, durch eine Abfrage zu einer Person auf einen Blick alle vorhandenen Informationen zu erhalten. Vielmehr muss er umständlich in den jeweiligen Datensystemen Abfragen und Recherchen tätigen und diese Erkenntnisse händisch zusammenführen, ganz zu schweigen von erforderlichen Recherchen in digitalen Beweismitteltöpfen, wie den Enchrochat-Daten. Das kann nicht der Anspruch an eine moderne Kriminalitätsbekämpfung sein.

Wir brauchen deshalb technische Lösungen wie das Auswerte- und Analysesystem VeRA, das bei der Polizei in Bayern eingeführt und über das Programm P 20 den Ländern zur Verfügung gestellt werden soll. Die Kernkompetenz von VeRA ist der direkte Zugriff und das Zusammenführen und Auswerten von Daten aus unterschiedlichen Quellen.

Das System kann bereits vorhandene polizeiliche Datenbestände verarbeiten, einen Datenabgleich von strukturierten sowie unstrukturierten Datenbeständen zum Erkennen von Zusammenhängen sowie geografische Auswertungen und die Visualisierung und den Export (mit Quellangaben) von Rechercheergebnissen sowie von Beziehungszusammenhängen zwischen Objekten durchführen. Durch Protokollierungsfunktionen kann der gesamte Bearbeitungsprozess gerichtsfest nachvollzogen werden.

Inwieweit diese Software zukünftig auch von der Polizei Hamburg genutzt werden kann, bedarf noch weiterer datenschutzrechtlicher Prüfungen; die grundsätzlichen rechtlichen Voraussetzungen sind in Hamburg durch die Änderungen des Polizeilichen Datenverarbeitungsgesetz geschaffen worden.

Ich bin mir aber der Kritik an dem amerikanischen Hersteller der Software bewusst und wir werden in Hamburg die Ergebnisse der Verfassungsbeschwerden mit Spannung abwarten.

Der diesjährige Sicherheitstag beschäftigt sich ja mit den Chancen, Risiken und regulativen Herausforderungen, vielleicht ein guter Zeitpunkt, auch über VERA zu diskutieren - Geht es doch um nicht weniger als den Zielkonflikt zwischen Freiheit und Sicherheit einer Gesellschaft im Zeitalter der digitalen Transformation.

Die Vorträge bilden dabei die gesamte Bandbreite zwischen den technischen Möglichkeiten, den fachlichen Anforderungen, aber auch den rechtlichen Rahmenbedingungen ab.

Sie zeigen aber auch auf, wie bedeutsam die Befassung mit dem Thema für die Zukunft einer erfolgreichen Kriminalitätsbekämpfung ist.

Künstliche Intelligenz – Gefahr oder Chance für unsere Sicherheit? Eine interdisziplinäre Auseinandersetzung am Beispiel von Deepfakes

Anna R. Louban[1]*, Milan Tahraoui*[2]

Anwendungen, die auf dem Einsatz von Künstlicher Intelligenz (KI) basieren, sind Teil unseres digitalen Alltags geworden. Sei es durch die Verwendung von Übersetzungsprogrammen (z.B. Deepl.com), die Einzug in die berufliche Kommunikationspflege gehalten haben, oder die Optimierung von privaten Fotografien, die unsere Smartphones durch Voreinstellung ausführen – der Gebrauch von KI-gestützten Programmen rückt täglich immer weiter in Richtung der Normalität und entzieht sich infolgedessen zunehmend einer kritischen Auseinandersetzung. Am Beispiel von Deepfakes, also KI-generierten oder -manipulierten Bildern und Videos, werden in diesem Beitrag die besonderen Herausforderungen für die Arbeit der Strafverfolgungsbehörden im Zusammenhang mit qualitativ hochwertigen und leicht zugänglichen KI-Anwendungen erörtert.

Die Strafverfolgungsbehörden sind mit der Aufgabe konfrontiert, die Echtheit von audiovisuellem Material prüfen zu können. In Abhängigkeit vom Sachverhalt gilt es nachzuweisen, dass digitales Material echt oder gefälscht ist. Beschlagnahmtes audiovisuelles Material gilt es in seiner Echtheit zu bestätigen. Bilder und Videos, die einer Manipulation unterzogen worden sind, um Betrugshandlungen vorzunehmen, müssen verlässlich als gefälscht klassifiziert werden können. Eine technische Lösung für die Prüfung audiovisuellen Materials auf Manipulation durch den Einsatz von Künstlicher Intelligenz sieht ihrerseits das Heranziehen von KI-basierten Systemen vor. Die Erforschung eines KI-basierten Deepfake-Detektors im Anwendungsfeld der nationalen Strafverfolgungsbehörden, wie sie im Forschungsprojekt FAKE-ID[3] vorgenommen wird, liefert hierzu Überlegungen aus interdisziplinärer Perspektive.

---

[1] Anna R. Louban erforscht die Thematik der Künstlichen Intelligenz aus sozialwissenschaftlicher Perspektive, u.a. im Kontext polizeilicher Anwendungen. Seit 2021 ist sie wissenschaftliche Mitarbeiterin im Forschungsinstitut für öffentliche und private Sicherheit (FÖPS) der Hochschule für Wirtschaft und Recht (HWR) und bearbeitet zwei BMBF-geförderte Forschungsprojekte mit KI-Bezug.

[2] Milan Tahraoui ist wissenschaftlicher Mitarbeiter am Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin) der Hochschule für Wirtschaft und Recht Berlin (HWR) und promoviert im internationalen Recht an der Paris 1 Pantheon-Sorbonne Universität und der Freien Universität Berlin.

[3] Dieser Beitrag entstand im Rahmen des Forschungsprojektes „FAKE-ID: Videoanalyse mit Hilfe künstlicher Intelligenz zur Detektion von falschen und manipulierten Identitäten“. Dieses Konsortialprojekt wird vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der Bekanntmachung Künstliche Intelligenz in der zivilen Sicherheitsforschung gefördert.

Deepfakes – verfälschte Videos, manipulierte Rezipient:innen

Die technische Definition von Deepfakes ist bislang nicht abschließend erfolgt.[4] Zuvorderst wird auf den Begriff Deepfakes zurückgegriffen, wenn darauf hingewiesen werden soll, dass Bilder, Texte, Videos oder Audiodateien mit Methoden des *Deep Learning*, hergestellt oder verändert worden sind. Auf diese Herstellungs- beziehungsweise Bearbeitungsweise nimmt auch der erste Teil (‚deep') der dem Englischen entliehenen Wortkomposition Deepfakes Bezug. Entsprechend handelt es bei Deepfakes stets um manipuliertes oder gänzlich synthetisch generiertes, digitales Material, das bei den Rezipient:innen den Anschein von echten Darstellungen erzeugt. Das Moment der Verfälschung weist der in Deepfakes integrierte englische Begriff ‚fake' aus, der etymologisch auf die Verben „vortäuschen, nachmachen" zurückgeführt wird.[5]

Die inhaltliche Vielfalt der Manipulationen, die digitales Material erfahren kann, ist bemerkenswert. Dargestellte Akteur:innen können ausgetauscht, präsentierte Ereignisse an andere Orte übertragen oder zeitliche Rahmungen von Geschehnissen verändert werden. Auch gänzlich fiktive Handlungsabfolgen erfundener Akteur:innen können mittels KI erzeugt und in Form von Deepfakes glaubwürdig präsentiert werden. Auf Details fokussierte Manipulationen, die durch Veränderungen einzelner Bereiche der Mimik, Gestik oder des sprachlichen Ausdrucks einer Person hergestellt werden, können ebenso überzeugend in digitales Material integriert werden. In der Konsequenz nehmen Rezipient:innen die betrachteten Darstellungen als echt wahr und handeln entsprechend. Insbesondere in Kontexten der politischen Entscheidungsfindung kann das problematisch sein.[6]

Deepfakes nehmen an (technischer) Qualität und Quantität zu

Einst erforderte die Herstellung von Deepfakes den Besitz tiefergreifender technischer Kenntnisse sowie die Verwendung kostenintensiver Soft- und Hardware. Mittlerweile können zahlreiche Programme gegen eine kleine Gebühr oder gar kostenfrei erworben werden, die qualitativ technisch hochwertige Deepfake-Bilder und -Videos erstellen können.[7] Die Bedienung dieser Software setzt kaum technisches Wissen voraus. Der technisch und monetär niedrigschwellige Zugang zur Produktion von synthetisch verändertem oder generiertem Videomaterial führt zu steigender Quantität von qualitativ zunehmend hochwerti-

[4] z.B. *Altuncu u.a.,* arXiv:2208.10913.
[5] https://www.duden.de/rechtschreibung/Fake (18.01.2023).
[6] *Louban u.a.,* in: Friedewald u.a. (Hrsg.), Künstliche Intelligenz, Demokratie und Privatheit, 2022, 265 ff.
[7] z.B. midjourney.com, avatarify.ai, deepfakesweb.com, myheritage.de.

geren Deepfakes, die im World Wide Web platziert und geteilt werden. Vor dem Hintergrund des kursierenden qualitätsvollen Bild- und Videomaterials und seiner dynamischen Verarbeitungsweise, wird das gesellschaftliche Nachdenken in Bezug auf ‚Wahrheit' und ‚Sicherheit' in Richtung technischer Möglichkeiten gerückt, insbesondere hinsichtlich der Möglichkeiten, (un)echtes digitales Material zu detektieren.

Content und Kontext

Bei der Bewertung von digitalem Bild- und Videomaterial zeigen sich zwei Kategorien vordergründig: Content und Kontext. Bild- und Videoprüfungen, die den Content fokussieren, gehen von einer technisch hergestellten Manipulation des Bildinhalts aus. In Entsprechung zur Annahme einer technisch herbeigeführten Veränderung des Inhalts, werden (ebenso) technische Lösungen für die Detektion solcher Bild- und Videobearbeitungen präferiert.[8] Im vorliegenden Beispiel der Deepfakes und der Deepfake-Detektion durch die Strafverfolgungsbehörden sind es Anwendungen der Künstlichen Intelligenz, die sowohl für die Herstellung der Content-Manipulationen verwendet werden, als auch für die Detektion audiovisueller Manipulationen herangezogen werden sollen.

Dass technische Detektionswege zumindest nicht ausschließlich zur Eindämmung von Deepfakes im Internet führen können, zeigt hingegen die Studie von Pennycook u.a., die sich mit der Frage des Kontexts auseinandersetzt. [9] Der Beitrag beleuchtet Kriterien, entsprechend derer Benutzer:innen sich entschließen, bestimmte Inhalte auf ihren Profilseiten zu teilen. In diesem Zusammenhang stellen die Autor:innen fest, dass bei dieser Entscheidung, nicht der (antizipierte) Wahrheitsgehalt von Inhalten maßgebend ist, sondern die Erwartung an Aufmerksamkeitsgenerierung für das eigene Profil.[10] Dieses Beispiel zeigt, dass eine ausschließlich technische Content-bezogene Auseinandersetzung zu kurz greift und kontextuelle Reflektionen der Verbreitung von KI-manipuliertem Material ebenfalls notwendig sind.

[8] Einen Überblick über aktuelle Studien zur Erkennung von gefälschten Inhalten mithilfe von Deep-Learning-Ansätzen gegeben *Passos u.a.*, arXiv:2202.06095.
[9] *Pennycook u. a.,* Nature 2021, 590.
[10] *Pennycook u. a.,* Nature 2021, 590.

Deepfakes – neues Thema (in) der Polizeiarbeit

Das Phänomen Deepfakes stellt ein aussagekräftiges Beispiel für die Herausforderungen dar, mit denen Strafverfolgungsbehörden hinsichtlich KI-Anwendungen konfrontiert sind. Einerseits gilt es im Rahmen von Polizeiarbeit Straftaten, die mit Einsatz von KI ausgeführt werden, aufzudecken. Ein Beispiel hierfür sind Manipulationen von digitalem Material, das zu Betrugszwecken eingesetzt wird. Erst vor kurzem wurde ein Fall des sogenannten ‚CEO-Frauds' (Chef-Betrug) publik, der einen wirtschaftlichen Schaden im zweistelligen Millionenbereich zur Folge hatte.[11] Die meisten Deepfakes im Internet gehören laut der Zählung von von Ajder u.a. im Jahr 2019 jedoch zur Kategorie der „non-consensual deepfake pornography".[12] Aus den insgesamt 14.678 Deepfakes, die die Studie online findet, stellen 96% pornographischen Inhalt dar, deren Erstellung die abgebildeten weiblichen Personen nicht zugestimmt haben.[13] In einer Online-Landschaft, die von misogynem „gendertrolling"[14] gezeichnet ist, verwundert es nicht, dass die an sich neutrale Technologie der Bildmanipulation regelmäßig in Form digitaler sexualisierter Gewalt gegen Frauen gerichtet wird.[15] Die Autor:innen Burkell und Gosse appellieren vor diesem Hintergrund für „a more material-based approach, opposed to technological, to understanding the harm presented by deepfakes."[16]

Anderseits nehmen die Möglichkeiten KI-assistierter Anwendungen innerhalb der Polizeiarbeit an Relevanz zu, nicht zuletzt, um Straftaten, die unter Verwendung Künstlicher Intelligenz begangen worden sind, effizienter verfolgen zu können. Vor dem Hintergrund großer digitaler Datenmengen, die die Strafverfolgungsbehörden hinsichtlich ihrer Aussage- und Beweiskraft prüfen müssen, erscheint eine semi-automatisierte technische Lösung für die Unterscheidung von Inhalten naheliegend. Über den erfolgreichen Einsatz einer KI-Anwendung zur Detektion von Material, das Missbrauchsabbildungen von sexualisierter Gewalt gegen Kinder enthält, berichtete Nordrhein-Westfalens Justizminister Peter Biesenbach.[17] Das im Forschungsprojekt[18] der Zentral- und Ansprechstelle Cybercrime

[11] *Hurst, Luke,* Binance executive says scammers created deepfake 'hologram' of him to trick crypto developers.
[12] *Ajder u. a.*, The State of Deepfakes, 2019.
[13] *Ajder u. a.*, The State of Deepfakes, 2019.
[14] *Mantilla*, Gendertrolling, 2015.
[15] *Mantilla*, Feminist Studies, 39 (2), 563; *Citron*, Yale Law Journal, *128* (7), 1870; *Jurasz*/*Barker*, German Law Journal 22 (5), 784; *Delfino*, Fordham Law Review, 88 (3), 887.
[16] *Burkell/Gosse*, First Monday, 24 (12).
[17] *ntv.de*, KI erkennt Kinderpornos zu über 90 Prozent, 2021.
[18] *Land.nrw*, Künstliche Intelligenz im Kampf gegen Kinderpornographie, 2019.