

Predictive Policing – die Polizeiarbeit der Zukunft?

von Laura Scholz



Open Peer Review

Dieser Beitrag wurde lektoriert von: Isabel Ecker, Clarissa Kupfermann und Christine Untch



Laura studiert Jura in Köln und macht derzeit ihren Schwerpunkt im internationalen Straf- und Strafverfahrensrecht. Ihre Interessen liegen besonders im Bereich der Anwendung von Legal Tech im Strafrecht.

A. Allgemeines

Predictive Policing bedeutet voraussehende Polizeiarbeit. Es ist aber – was fälschlicherweise manchmal unterstellt wird – gerade keine Vorhersage der Zukunft. Die Möglichkeit der Berechnung von zukünftigen Ereignissen mag auf den ersten Blick zwar futuristisch klingen, ist aber bereits in der Gegenwart möglich.

Warum die Beschreibung von Predictive Policing als vorhersagende Polizeiarbeit ungeeignet ist, zeigt bereits eine nähere Betrachtung der zur Umsetzung verwendeten Systeme. So werden gerade nicht – wie etwa in Science-Fiction-Filmen – Straftaten vorhergesagt, sondern lediglich die Wahrscheinlichkeit für deren Eintritt berechnet. Eine einheitliche Definition für Predictive Policing findet sich nicht. Häufig wird es als die Anwendung analytischer Verfahren definiert, die anhand statistischer Prognosen potenzielle Vorfälle von Kriminalität identifizieren sollen. Hierfür

werden algorithmische Systeme verwendet, um die Wahrscheinlichkeit der Begehung einer Straftat an einem spezifischen Ort zu einer bestimmten Zeit zu berechnen. Auf diese Verbrechensprognosen können Polizeibeamte präventiv reagieren und etwa ihre Präsenz in den betroffenen Gebieten erhöhen. Software soll Muster in großen, vergangenheitsbezogenen Datenmengen erkennen, welche auf zukünftige Kriminalitätsereignisse hindeuten könnten. Es handelt sich beim Predictive Policing daher keinesfalls um definitive, stichhaltige Prognosen, wie etwa im Film *Minority Report*, vielmehr liegt der Schwerpunkt auf errechneten Wahrscheinlichkeiten.

Das Ziel des Einsatzes von Predictive-Policing-Software ist in erster Linie die Prävention, also die Gefahrenabwehr. Doch auch zur Aufklärung vergangener Taten können die Erkenntnisse aus den Prognoseberechnungen genutzt werden.

B. Die technische Umsetzung

Doch wie funktioniert Predictive Policing genau? Zu unterscheiden ist zunächst zwischen orts- und personenbezogenem Algorithmen. Software, die mittels umfassender Datenanalysen prognostiziert, wo sich zukünftig Tatorte befinden könnten, sind Teil des ortsbezogenen Predictive Policing. Analysen können sich jedoch auch darauf beziehen, welche Personen zukünftig mutmaßlich straffällig werden könnten (personenbezogenes Predictive Policing). Zu den verwendeten Daten zählen etwa vergangene Tatorte, -zeiten und -hergänge; bei personenbezogenen Systemen auch viele weitere soziale Umstände wie Alter, Geschlecht und Einkommen des potenziellen Täters. Die gesammelten Datenmengen werden in einen meist lernfähigen Algorithmus eingespeist, der die Wahrscheinlichkeiten des Eintritts von Straftaten errechnet. Als Grundlage für zuverlässige Prognosen werden jedoch sehr große Datenmengen benötigt, wobei Qualität, Aktualität und Verfügbarkeit dieser Datenbasis eine große Rolle spielen. Je aktueller und aussagekräftiger die auszuwertenden Daten sind, desto verlässlicher werden die Prognosen. Es muss daher fortlaufend sichergestellt werden, dass die Datenbasis qualitativ ist und bei Bedarf verbessert wird.

Die meiste Predictive-Policing-Software arbeitet mit Big-Data-Analytics, welche die Verwertung besonders großer Mengen an in der Vergangenheit erhobenen Kriminaldaten ermöglicht.

Hierbei werden beispielsweise signifikante Abweichungen und Auffälligkeiten grafisch dargestellt, die auf zukünftige Straftaten hindeuten könnten. So könnten Wohngebiete, in denen zuvor häufiger eingebrochen wurde, bildlich hervorgehoben werden.

Zur Berechnung der Wahrscheinlichkeiten werden verschiedene Methoden eingesetzt, wobei die sogenannte Near-Repeat-Theorie eine große Rolle spielt. Dieser Ansatz geht davon aus, dass Verbrechen häufig in der Nähe von Orten geschehen, wo bereits in der Vergangenheit vermehrt Straftaten geschehen sind. Es wird hierbei ferner davon ausgegangen, dass potenzielle Täter die Risiken, aber auch die Erfolgschancen ihrer Taten in der Umgebung von Tatorten am besten einschätzen können und daher vorzugsweise in jenen „bekannten Gefilden“ bleiben. Insbesondere Software, die für die Berechnung von Wahrscheinlichkeiten eines bevorstehenden Wohnungseinbruchs eingesetzt wird, basiert oft auf dieser Theorie, da sie sich für diesen Bereich bereits in einigen Studien als zuverlässig gezeigt hat. Einher mit der Near-Repeat-Theorie geht auch das kriminologische Konzept der Repeat Victimisation, wobei davon ausgegangen wird, dass zum Nachteil einer Person, die bereits Opfer einer Straftat wurde, eine erneute Begehung wahrscheinlicher erscheint. Erweitert wird dieser Ansatz meist durch eine räumlich-temporale Analyse, die auch eine etwaige Schätzung des potenziellen Tatzeitpunktes ermöglichen kann, sodass die Polizei etwa ihre Streifen zu diesen Zeitpunkten gezielt erhöhen kann. Nach diesen Theorien betrachten die Algorithmen folglich wo, gegenüber wem und wann die Straftaten begangen wurden.

Ein weiterer Ansatz ist die Risk-Terrain-Analyse. Mithilfe dieser werden auch sozioökonomische und infrastrukturelle Merkmale einbezogen. Damit lassen sich positive Korrelationen zwischen dem Auftreten bestimmter Merkmale wie etwa hohem Einkommen, guter Verkehrsanbindung und dem Auftreten von bestimmten Delikten – wie beispielsweise Einbruchsdiebstählen – herstellen. Umgebungen, die diese Merkmale aufweisen, werden nach diesem Ansatz schließlich als potenziell von Kriminalität betroffen eingestuft.

Dies geschieht oft im Zusammenspiel mit neuronalen Netzwerken, welche die Struktur eines menschlichen Gehirns in gewisser Hinsicht nachbilden sollen.

Dem zwar ähnlich, jedoch auf die Erstellung von Mustern aufgrund von gemessenen Entfernungen fokussiert, ist der statistische Modeling-Ansatz. Hierbei wird die Distanz zwischen potenziellen Tatorten und geografischen Besonderheiten wie Autobahnauffahrten oder abgelegenen Waldstraßen von einem Algorithmus verglichen. Findet der Algorithmus ein bestimmtes Muster dieser Entfernungen, können auf dieser Grundlage ebenfalls Aussagen über wahrscheinliche Kriminalität getroffen werden.

C. Wie und wo wird Predictive Policing heute angewendet?

In Deutschland wird Predictive Policing bereits seit ca. fünf Jahren probeweise angewendet, wobei der Schwerpunkt deutlich auf ortsbezogener Software liegt. Meist werden diese vor allem zur Prävention von Wohnungseinbrüchen, Gewerbeeinbrüchen oder Kfz-Diebstählen verwendet. Personenbezogene Algorithmen werden etwa in den USA, in der Schweiz und in China angewendet, wo das Datenschutzrecht weniger restriktiv als das Deutsche scheint. In den USA werden auch Autokennzeichen, Meldedaten sowie Facebookposts in die Datenanalyse einbezogen. Die Risiken der Anwendung solcher personenbezogenen Predictive-Policing-Software sind das damit einhergehende Diskriminierungspotenzial – Stichwort: Racial Profiling – aber auch massive Eingriffe in die Persönlichkeits- und Datenschutzrechte. Diese Gründe stehen einer der USA vergleichbaren Anwendung in Deutschland bisher entgegen. Trotz dieser Bedenken werden in einigen wenigen deutschen Bundesländern, darunter Hessen, solche Algorithmen erprobt. Das Projekt *Hessendata* wird ausschließlich zur Terrorbekämpfung eingesetzt. Das Ziel hierbei ist es, die Radikalisierung einzelner Personen möglichst frühzeitig zu erkennen.

In NRW wird Predictive Policing etwa für die Berechnung der Wahrscheinlichkeit von Wohnungs- und Gewerbeeinbrüchen verwendet. Seit 2015 ist hier das „System zur Kriminalitätsauswertung und Lageantizipation“ (*SKALA*) im Einsatz. Dieses soll dazu dienen, die zielgerichtete und

strategische Polizeiarbeit zu verbessern, indem aufkommende Brennpunkte auf Basis kriminalitätsrelevanter Faktoren frühzeitig identifiziert werden. Seit dem 01.01.2021 steht *SKALA* zur Kriminalitätsprognose flächendeckend allen Kreispolizeibehörden in NRW zur Verfügung. Das Programm soll die Polizei bei der Einsatzplanung unterstützen. Die Prognosen beziehen sich auf die Einbruchswahrscheinlichkeit für jeden Wohnbezirk einer zuständigen Polizeibehörde, aber auch auf Gewerbeobjekte und Delikte im Zusammenhang mit Fahrzeugen, wie etwa der Diebstahl von Airbags oder Navigationsgeräten. Ist das Risiko für ein Gebiet erhöht, wird dies im Visualisierungs- und Auswertungstool *SKALA/MAP* dargestellt, sodass die Polizei hier entsprechende Maßnahmen, wie beispielsweise erhöhte Streifenfahrten, treffen kann.

Andere Bundesländer wie Bayern und Baden-Württemberg nutzen ähnliche Software, darunter etwa die auf der Near-Repeat-Theorie basierende Software *PRECOBS* oder darauf aufbauende, weiterentwickelte Systeme wie *PreMaps* in Niedersachsen.

D. Fazit

Predictive Policing soll die Kriminalität minimieren; im besten Fall sogar verhindern. Das Problem des Einsatzes liegt jedoch darin, dass man nie wissen kann, ob es tatsächlich zu einer errechneten Straftat gekommen wäre und somit den Erfolg solcher Software kaum messen kann. So kann eine berechnete Straftat entweder aufgrund einer erhöhten Polizeipräsenz ausgeblieben sein oder sie wäre ohnehin nie geschehen. Wegen dieser Ungewissheit ist eine Bezifferung des Erfolges von Predictive Policing kaum messbar. Auch könnten sich Tatorte lediglich verlagern. Da die Analysen von der hohen Qualität der Datenbasis abhängig sind, muss zudem kostspielig sichergestellt werden, dass diese immer aktuell ist und möglichst qualitativ hochwertig zur Verfügung steht.

Im Film *Minority Report* wird zum Beispiel ein Mann verhaftet – für einen Mord, den er mutmaßlich erst einige Zeit nach der Festnahme begehen würde. Solche Szenarien sind rein fiktional und sind weder mit gängiger personenbezogener Software noch mit den in Deutschland verwendeten Systemen vergleichbar.

Diese stellen nicht etwa einen Paradigmenwechsel der praktischen Polizeiarbeit dar, sondern ergänzen diese lediglich als effizienzsteigerndes Hilfsmittel. In Europa und insbesondere Deutschland ist mit einer Anwendung derartiger personenbezogener Predictive-Policing-Systeme – wie es in den USA bereits geschieht – auf längere Sicht nicht zu rechnen, da stets das Verhältnis zwischen öffentlicher Sicherheit und Beachtung der verfassungsrechtlich geschützten Persönlichkeitsrechte aufrechterhalten werden muss.

Weiterführende Hinweise:

Kupfermann, Was ist Machine Learning?, CTRL 1/2021, https://legaltechcologne.de/wp-content/uploads/2021/02/Cologne-Technology-Review-Law_CTRL_1-21_Clarissa-Kupfermann_Was-ist-Machine-Learning.pdf (Stand: 01.06.2021).

Knobloch, Chancen und Gefahren von Predictive Policing, <https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/predictive.policing.pdf> (Stand: 01.06.2021).

Simmler, Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege, <https://www.alexandria.unisg.ch/262339/1/Predictive%20Policing%20-%20Grundlagen%2C%20Funktionsweise%20und%20Wirkung.pdf> (Stand: 01.06.2021).

Povalej/Volkman, Überblick Predictive Policing, <https://link.springer.com/content/pdf/10.1007/s00287-021-01332-4.pdf> (Stand: 01.06.2021).

Gerstner, Predictive Policing und Wohnungseinbruch, https://pure.mpg.de/rest/items/item_2498917/component/file_3014304/content (Stand: 01.06.2021).

Sommerer, Personenbezogenes Predictive Policing, https://www.researchgate.net/publication/343263377_Personenbezogenes_Predictive_Policing_-_Kriminalwissenschaftliche_Untersuchung_uber_die_Automatisierung_der_Kriminalprognose (Stand: 01.06.2021).

CTRL

Cologne Technology **R**&Law
review

+
Hier geht es zur
ganzen Ausgabe.

Dort findest du auf über
100 Seiten in 15 Aufsätzen
alles von NFTs über Legal
Tech im Strafprozess bis
hin zum Stand des
E-Examens in NRW.

