

Predictive Policing: Umsicht ist geboten

Datengestützte Analyseverfahren können die Wirksamkeit und Effizienz von Polizeiarbeit erhöhen. Polizeidepartemente sollten allerdings beim Einsatz solcher Verfahren Umsicht walten lassen, um Risiken in Bezug auf Grund- und Freiheitsrechte zu vermeiden.

Von Matthias Leese

Datengestützte Analyseverfahren wie beispielsweise *Predictive Policing* fanden in den letzten Jahren weit- hin Beachtung. Mittels algorithmenbasierter Analyse von Kriminaldaten identifiziert *Predictive Policing*-Software mögliche Kriminalitätsrisiken und versetzt Polizeidepartemente so in die Lage, Präventionsmassnahmen zielgerichtet einzusetzen. Polizeiarbeit kann auf diese Weise wirksamer und effizienter gestaltet werden. So können Ressourcen eingespart werden. Vor allem im Hinblick auf Budgetkürzungen in vielen Bereichen von Verwaltung und öffentlichem Dienst hat diese Argumentation grossen Anklang gefunden.

Eine neue Studie, die am Center for Security Studies, an der Universität Hamburg und an der Technischen Universität Berlin durchgeführt wurde, hat nun zum ersten Mal umfassend untersucht, wie die Anwendung von *Predictive Policing*-Software Polizeiarbeit verändert. Basierend auf mehrjähriger Feldforschung analysiert die Studie unter anderem, welche Auswirkungen datengestützte Analyseverfahren auf Grund- und Freiheitsrechte, sowie auf das Verhältnis zwischen der Polizei und der Bevölkerung haben können.

Die Datengrundlage der Studie umfasst Experteninterviews mit PolizeibeamtInnen, KriminalanalytInnen und SoftwaredesignerInnen, sowie teilneh-

mende Beobachtungen bei der Kriminalanalyse mit *Predictive Policing*-Software. Hinzu kam die verfügbare technische, operative und rechtliche Dokumentation im Hinblick auf *Predictive Policing*. Der resultierende Datenkorpus wurde systematisch codiert und nach relevanten Themenbereichen sortiert. Auf diese Weise wurde ein Überblick über die dringlichsten Fragen und Herausforderungen bei der datengestützten Polizeiarbeit erstellt.

Die Ergebnisse der Studie bildeten die Grundlage für das Buch *Criminal Futures: Predictive Policing and Everyday Police Work*, das gemeinsam von Matthias Leese

Schlüsselaussagen

- ! Datengestützte Analyseverfahren können bei der Verbrechensprävention helfen.
- ! Technologien wie *Predictive Policing* bergen jedoch gleichzeitig potenzielle Gefahren für Grund- und Freiheitsrechte und können sich negativ auf das Verhältnis zwischen Polizei und Bevölkerung auswirken.
- ! Um einen verantwortungsbewussten Einsatz von datengestützten Analyseverfahren sicherzustellen, sollten Polizeidepartemente Fragen von Daten, Automatisierung, Entscheidungsfindung, Kommunikation und operativen Massnahmen kritisch reflektieren.



Ein Polizeibeamter in Chicago überwacht die Beobachtungsgeräte der Polizei.
Joshua Lott / Reuters

und Simon Egbert verfasst wurde (Routledge 2021). Das Buch ist als Open Access [eBook Version](#) zum freien Download verfügbar. Die vorliegende Policy Perspective fasst die wichtigsten Empfehlungen des Buchs für einen verantwortungsbewussten Einsatz von datengestützten Analyseverfahren in der Polizeiarbeit zusammen.

Ein verantwortungsbewusster Einsatz von datengestützten Analyseverfahren: 7 Schritte

Erstens: Daten sollten nicht als ein «wahres» Abbild der Welt missverstanden werden. Sie stellen immer eine selektive Perspektive dar, die im Hinblick auf spezifische Verwendungskontexte produziert wurde. Eine gesunde Skepsis Daten gegenüber ist daher angebracht, insbesondere, wenn Daten aus externen Quellen stammen.

Daten existieren niemals unabhängig von ihrer Produktion. Wenn PolizeibeamtInnen Kriminaldaten an einem Tatort sammeln, dann suchen sie nach spezifischen Merkmalen, die es ihnen erlauben, den vorliegenden Tatbestand zu beschreiben und zu katalogisieren. Die Kategorien für Kriminaldaten sind dabei schon im Vorfeld durch das Klassifikationsschema der Datenbank festgelegt, deren Teil sie im späteren Verlauf werden. Beobachtungen, die nicht diesem Schema entsprechen, werden nicht Teil des produzierten Datensatzes. Schon die Datengenerierung beinhaltet also zwangsläufig immer eine Auswahl.

Darüber hinaus können bei der Datengenerierung Fehler passieren. Am Tatort können Dinge übersehen werden, es können sich Ungenauigkeiten bei der Dateneingabe einschleichen oder Beobachtungen können falsch klassifiziert werden.

Ein weiterer wichtiger Aspekt in Bezug auf Kriminaldaten ist ihre Volatilität. Gerade zu Beginn von Ermittlungen ist häufig noch kein kohärentes Bild von Tathergang,

Diebesgut, Sachschäden, verdächtigen Personen oder forensischen Untersuchungen vorhanden. Wenn sich im Verlauf der Zeit neue Erkenntnisse ergeben, müssen Daten zeitnah und regelmässig aktualisiert werden. Kriminaldaten gelten als notorisch unzuverlässig und müssen strengen Qualitätskontrollen unterzogen werden.

Zusammenfassend unterliegt jeder Datensatz – und das gilt auch für Datensätze aus externen Quellen – Selektionsmechanismen. Diese Tatsache liegt in der Sache der Natur, sollte aber bedacht werden, wenn es um den «Wahrheitsgehalt» von Daten und darauf basierender Analysen geht. Im Fall von *Predictive Policing* können fehlerhafte Daten beispielsweise zu fehlerhaften Risikoprognosen führen.

Zweitens: Datengestützte Analyseverfahren sollten jederzeit transparent und nachvollziehbar sein, unabhängig davon, ob es sich um kommerzielle Produkte oder behördliche Eigenentwicklungen handelt. Übermässig komplexe und nicht nachvollziehbare Verfahren können sich negativ auf die Fähigkeit von Polizeidepartementen auswirken, Rechenschaft über ihre Tätigkeiten abzulegen. Zudem können sie zu Widerstand seitens des ausführenden Personals führen.

Algorithmen können einfach und leicht verständlich sein. Sie können allerdings auch hochkomplexe Verfahren darstellen, die selbst für ExpertInnen kaum mehr nachvollziehbar sind, insbesondere, wenn Formen von maschinellem Lernen involviert sind. Solche komplexen Algorithmen werden häufig dazu eingesetzt, grosse und heterogene Datensätze zu analysieren.

Aufgrund ihrer Undurchsichtigkeit werden solche Algorithmen gemeinhin als *black boxes* bezeichnet. Der Nutzer kann zwar sehen, welche Daten in das System eingespeist und welche Ergebnisse produziert werden, aber den dazwischenliegenden analytischen Prozess nicht mehr nachvollziehen. Die Wahrscheinlichkeit, dass datengestützte Analyseverfahren solche *black boxes* beinhalten, steigt zusätzlich, wenn kommerzielle Software verwendet wird, deren Innenleben vom Hersteller aus Wettbewerbsgründen nicht offengelegt wird.

Für die Polizeiarbeit haben *black boxes* zwei wichtige Konsequenzen. Erstens können sie die Fähigkeit von Polizeidepartementen untergraben, der Öffentlichkeit gegenüber Rechenschaft für ihr Handeln abzulegen. Rechenschaftsfähigkeit fusst darauf, Entscheidungen erklären zu können. Wenn diese Entscheidungen allerdings auf für Menschen nicht nachvollziehbare Art und Weise zu Stande kommen, dann wird dies zu einem Problem.

Zweitens machen *black boxes* interne Widerstände innerhalb von Polizeidepartementen wahrscheinlicher. PolizeibeamtInnen sind traditionell skeptisch gegenüber neuen Technologien eingestellt. Diese Skepsis kann in of-

fenen Widerstand umschlagen, wenn BeamtInnen das Gefühl bekommen, dass ihre eigene professionelle Expertise und Erfahrung von Analyseverfahren abgelöst wird, die nicht nachvollzogen werden können.

Drittens: Eine vollständige Automatisierung von Analyseprozessen sollte ausgeschlossen werden. Der Mensch muss immer in den Prozess eingebunden bleiben und die Kontrolle über das System behalten. Das bedeutet, dass das System keine Informationen zurückhalten oder kritische Entscheidungen ohne Einwilligung des Nutzers treffen darf.

Predictive Policing-Software und andere datengestützte Analyseverfahren automatisieren viele der Prozesse, die vorher von menschlichen AnalystInnen ausgeführt wurden. So können Ergebnisse schneller, auf der Grundlage grösserer Datenmengen und nicht zuletzt frei von Verarbeitungsfehlern produziert werden. Automatisierung bildet die Grundlage für viele Vorteile von datengestützter Analyse bei der Polizeiarbeit.

Ein Übermass an Automatisierung kann sich jedoch negativ auf die menschliche Kontrolle auswirken. So kann zu starke Automatisierung dazu führen, dass menschliche AnalystInnen bloss noch eine Zuschauerrolle im Analyseprozess bekleiden und im Zweifelsfall – wenn etwa Bedenken in Bezug auf Datenqualität oder operative Handlungsempfehlungen bestehen – nicht mehr eingreifen können.

Auf diese Weise können fundamentale Probleme im Hinblick auf Verantwortung und Rechenschaftsfähigkeit von Polizeidepartementen entstehen. Es ist daher wichtig, den Grad von Automatisierung bei datengestützten Analyseverfahren so zu kalibrieren, dass menschliche Kontrolle über Prozesse zu jedem Zeitpunkt gegeben ist.

Viertens: Entscheidungen dürfen nur von menschlichen AnalystInnen getroffen werden. Mit Blick auf automation bias sollte ein kritisches Hinterfragen von datengetriebenen Handlungsempfehlungen zudem ermutigt und die Möglichkeit eines menschlichen Vetos gegen das System institutionell verankert werden.

Die Forschung hat gezeigt, dass Menschen in der Zusammenarbeit mit Computersystemen einem sogenannten *automation bias* unterliegen, d.h. dass sie Handlungsempfehlungen des Systems tendenziell unkritisch folgen. Der Grund hierfür ist, dass Menschen technischen Systemen oft Objektivität, Neutralität und Fehlerfreiheit unterstellen.

Bei datengestützten Analyseverfahren lauern jedoch zahlreiche potenzielle Fehlerquellen, etwa bei Datengenerierung, Datenkonsolidierung und –aufbereitung, theoretischen Annahmen und

Modellierungen oder der Operationalisierung von Variablen. Blindes Vertrauen in algorithmisch erstellte Handlungsempfehlungen kann zu ebenfalls fehlerhaften operativen Entscheidungen führen, die die Effektivität von Polizeiarbeit und das Verhältnis zwischen Bevölkerung und Polizei negativ beeinträchtigen können.

Um informierte und verantwortungsbewusste Entscheidungen treffen zu können, sollten AnalystInnen ermutigt werden, sich kritisch mit allen Elementen des datengestützten Analyseprozesses auseinanderzusetzen und es sollte ihnen explizit das Recht eingeräumt werden, sich über Empfehlungen der Software hinwegzusetzen.

Fünftens: Die Kommunikation von datengestützten Analyseergebnissen sollte explizit betonen, dass ein Unterschied zwischen Risikoprognosen und Fakten besteht. Risikoprognosen, selbst wenn ihre Darstellung diesen Anschein erweckt, bedeuten nicht, dass innerhalb der prognostizierten Parameter tatsächlich Delikte stattfinden werden.

Datengestützte Analyseverfahren werden überwiegend in Präventionskontexten eingesetzt, wo sie Aufschluss über Kriminalitätsrisiken geben können. Auf der Basis von solchen Risikoeinschätzungen können Polizeidepartemente dann entscheiden, wo operative Massnahmen im Zuge von Präventionsstrategien am sinnvollsten eingesetzt werden können.

Es besteht dabei jedoch die Gefahr, dass Risikoeinschätzungen als Fakten missverstanden werden können. Das prognostizierte Kriminaldelikt – etwa ein Wohnungs-

Weiterführende Literatur

Egbert S. / Leese M., ***Criminal Futures: Predictive Policing and Everyday Police Work*** (London/New York: Routledge, 2021).

Dieses Buch fasst die Ergebnisse einer mehrjährigen empirischen Studie zu *Predictive Policing* in der Schweiz und in Deutschland zusammen. Die Analyse ist eingebettet in grössere theoretische, konzeptionelle und normative Überlegungen bezüglich datengestützter Analyseverfahren in der Polizeiarbeit.

Kaufmann M. / Egbert S. / Leese M., **«Predictive Policing and the Politics of Patterns»**, in: *British Journal of Criminology* 59:3 (2019), S. 674–692.

Dieser Artikel entwickelt ein theoretisches Verständnis von *Predictive Policing* und anderen datengestützten Analyseverfahren, die auf Mustererkennung beruhen. Die Arbeit wurde 2019 mit dem Radzinowicz-Preis für den wichtigsten wissenschaftlichen Beitrag im Themenfeld von Strafjustiz und Kriminologie ausgezeichnet.

Egbert S., **«Siegeszug der Algorithmen? Predictive Policing im deutschsprachigen Raum»**, in: *Aus Politik und Zeitgeschichte* 67:32-33 (2017), S. 17–23.

Dieser Artikel bietet einen Überblick über *Predictive Policing*-Verfahren und ihren Einsatz in der Schweiz und Deutschland.

einbruchdiebstahl – muss nicht zwangsläufig innerhalb der erwarteten räumlichen und zeitlichen Parameter eintreten. Es ist im Gegenteil sogar möglich, dass das Delikt auch ohne zielgerichtete Präventionsmassnahmen nicht stattfinden würde.

Die Tatsache, dass prognostizierte Delikte eintreten können oder auch nicht sollte bei der operativen Planung von Kriminalprävention explizit berücksichtigt werden, einschliesslich eines Bewusstseins der Bedeutung von Risiko und klarer Kommunikation. Auf diesem Wege können zielgerichtete Präventionsmassnahmen sinnvoll mit randomisierten und ungerichteten Massnahmen kombiniert werden.

Sechstens: Risikoprognosen können performative Effekte auf individuelles Verhalten entwickeln. Speziell Patrouillenkräfte sollten ein Bewusstsein dafür entwickeln, wie ihre eigene Wahrnehmung vom Wissen über Kriminalitätsrisiko geleitet sein kann und wie sich gesteigertes Misstrauen auf die Interaktion mit der Bevölkerung auswirken kann.

Wenn sie ihre Aufgaben auf der Grundlage von datenbasierten Risikoprognosen verrichten, zeigen Patrouillenkräfte eine Tendenz zu erhöhtem Misstrauen. In Quartieren mit einem vermeintlich höheren Kriminalitätsrisiko kann es entsprechend zu verstärkten Überwachungs- und Kontrollpraktiken kommen.

Dies kann Situationen beinhalten, in denen BürgerInnen als verdächtig empfunden werden, nur, weil sie sich in einem deklarierten Risikogebiet aufhalten. Verstärkte Überwachungs- und Kontrollmassnahmen, die lediglich auf generalisierten Risikoprognosen beruhen, verletzen jedoch das Prinzip eines begründeten Anfangsverdachts für Kontrollen. Besonders problematisch wird ein solches Verhalten, wenn es zu einer Verschärfung von bereits bestehenden Vorurteilen oder rassistischen Ansichten führt.

Es ist daher wichtig, Patrouillenkräften explizit zu vermitteln, dass eine Risikoprognose nicht zwangsläufig dazu führt, dass die vorhergesagten Delikte in einem Quartier wirklich stattfinden. Patrouillenkräfte sollten zudem mögliche performative Effekte kritisch reflektieren.

Siebtens: Die Potentiale und Limitationen von Predictive Policing und anderen datengestützten Analyseverfahren müssen sorgfältig evaluiert werden. Sie sollten im Opti-

malfall eine unterstützende Rolle einnehmen, nicht aber langfristige Strategien zur Ursachenbekämpfung von Kriminalität ersetzen.

Polizeidepartemente sollten auf der strategischen Ebene datengestützten Analyseverfahren keine übermässig grosse Rolle einräumen. Gerade vor dem Hintergrund von politischem Diskurs, Medienaufmerksamkeit und den Kosten für Beschaffung und Implementierung von Software gilt es, einer naheliegenden Nutzenmaximierung von technologischen Werkzeugen zu widerstehen.

Datengestützte Analyseverfahren sind dazu geeignet, Kriminalität präventiv zu unterdrücken, nicht jedoch, die eigentliche Entstehung von Kriminalität zu verstehen und damit Möglichkeiten zu bieten, Anreize für kriminelles Verhalten zu reduzieren. Die sozialen und ökonomischen Ursachen von Kriminalität liegen zwar in der Regel ausserhalb des Zuständigkeitsbereichs der Polizei. Nichtsdestotrotz ist es wichtig, dass technologische Lösungen keine langfristigen sozialen Strategien und gesellschaftlichen Debatten ersetzen können.

Zusammenfassung

Die hier vorgestellten Empfehlungen stehen beispielhaft für einige der dringendsten Fragen, die der Einsatz von datengestützten Analyseverfahren in der Polizeiarbeit aufwirft. Sie können Polizeidepartementen dabei helfen, ihre eigene Position kritisch zu hinterfragen und zu evaluieren, wie *Predictive Policing*-Software und andere datengestützte Verfahren verantwortungsbewusst eingesetzt werden können.

Die Bedürfnisse von Zivilgesellschaft und Polizeiorganisationen müssen dabei nicht zwangsläufig im Widerspruch zu einander stehen. Es bedarf allerdings einer gewissen Umsicht, um neue Technologien so einzusetzen, dass beide Seiten profitieren. Das gilt sowohl für bereits eingesetzte Verfahren wie auch für kommende Generationen von Datenanalyse.

Dr. Matthias Leese ist Senior Researcher am Center for Security Studies (CSS).

Die **Policy Perspectives** werden herausgegeben vom Center for Security Studies (CSS) der ETH Zürich. Das CSS ist ein Kompetenzzentrum für schweizerische und internationale Sicherheitspolitik.

Herausgeberin: Annabelle Vuille
Redaktion: Oliver Thränert, Niklas Masuhr
Layout: Miriam Dahinden-Ganzoni

Feedback und Kommentare: PolicyPerspectives@sipo.gess.ethz.ch
Weitere Ausgaben und Abonnement:
css.ethz.ch/en/publications/css-policy-perspectives

Zuletzt erschienene Ausgaben:

China's Rise Can Unite NATO (8/13)
Europe's Fiery Future: Rethinking Wildfire Policy (8/12)
US Evangelicals: From Prophecy to Policy (8/11)
Arms Control: For and By Europe (8/10)
Das Krisenmanagement kann aus der Krise lernen (8/9)
Keeping the Skies Open over Europe (8/8)

© 2020 Center for Security Studies (CSS), ETH Zürich
ISSN: 2296-0244; DOI: 10.3929/ethz-b-000453441