

# Unterschätzte Gefahr: Künstliche Intelligenz zur Verbrechensprognose

Von Andreas von Rényi

Quelle: KOPP-exklusiv Nr. 45/2017

**Aus Fiktion soll Realität werden. Strafverfolger wollen Verbrechen per Computer-Algorithmus vereiteln, bevor sie geschehen. Die Dokumentation *Pre-Crime* sorgt derzeit für Furore. Tatsächlich wird die neue Sicherheitstechnologie selbst zur Gefahr für den Bürger.**

Man könnte meinen, da habe jemand zu oft *Minority Report* geschaut und sich hoffnungslos in einer Science-Fiction-Welt verloren: Neue Technologien sollen nun zunehmend ermöglichen, Verbrechen vorherzusagen und zu vereiteln, alles völlig real. Und schon im Film ganz großes Kino.

- *Der Spielberg-Streifen aus dem Jahr 2002 versetzt den Konsumenten ins Jahr 2054. In dieser noch recht fernen Zukunft existiert in Washington eine Sonderabteilung, die mittels dreier helllichtiger Medien und deren präkognitiver Fähigkeiten in der Lage ist, bevorstehende Morde rechtzeitig zu verhindern. Die künftigen Täter werden identifiziert und anschließend in künstliche Bewusstlosigkeit versetzt. Ein Prozess findet gar nicht erst statt. Die fiktive Handlung mündet in die Einsicht, dass nicht alle vorab überführten Personen tatsächlich ein Verbrechen begehen würden. Somit scheitert das gesamte Programm.*

Der längst nicht mehr so fiktive Spielfilm basiert auf einer bereits 1956 publizierten Kurzgeschichte des US-amerikanischen Autors *Philip Kindred Dick*. Er prägte den Begriff *Precrime* als Name für eine imaginäre Behörde, die Personen verhaftet, weil sie zu einem späteren Zeitpunkt ein Verbrechen begehen werden. Seit 1956 sind wir dem Jahr 2054 wesentlich näher und der *Precrime-Vision* sogar erschreckend nahe gekommen. Jetzt, im Jahr 2017, wollen sich Behörden nicht auf Präkognition verlassen, sondern bauen auf komplexe Formeln, Computer-Algorithmen und deren Situationsanalyse für potenziell bevorstehende Verbrechen. Doch was sich hier derzeit abspielt, erweist sich als unkontrollierbare Bedrohung.

## Die digitale Glaskugel

Moderne Verbrechensbekämpfung lebt von Big Data und Rechnerkapazität. Heute nun ist *Precrime* als Prinzip eine unübersehbare Tatsache, eine Erweiterung von Konzepten wie Rasterfahndung und Profiling. Die Analysetechnologie geht dabei von sehr logisch klingenden Annahmen und riesigen Datenmengen aus, um Präventionsarbeit zu ermöglichen. Ermittler greifen auf Erfahrungswerte und Statistiken zurück, befragen inhaftierte Straftäter zu ihren Gewohnheiten, um Wahrscheinlichkeiten künftiger Taten abzuschätzen und theoretische Modelle zu entwickeln.



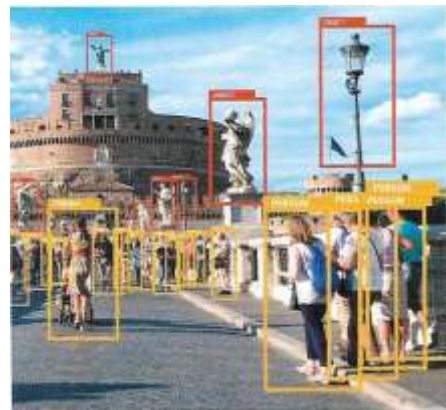
Die Grundprinzipien sind eher simpel. Stichwort *Viktimisierung*:

- Hat beispielsweise schon ein Einbruch in ein bestimmtes Gebäude stattgefunden, tendiert die Mehrzahl der Täter dazu, dasselbe Objekt erneut als Ziel zu wählen. Je häufiger sich dies wiederholt, desto größer wird die Wahrscheinlichkeit für eine baldige weitere *Viktimisierung*. Verschiedene Theorien definieren die Elemente, die überhaupt erst eine Straftat bedingen. Wird auch nur ein Element wirksam ausgeschaltet, kann die Tat nicht stattfinden. Motiv, Opfer und mangelnder Schutz sind drei wesentliche Faktoren. Während eine Theorie sich vor allem auf die Täterperspektive fokussiert, befasst sich eine andere vorwiegend mit dem Tatobjekt und den besonderen Eigenschaften, die es als Ziel prädestinieren. Doch wird diese Simplifikation nicht der aktuellen Methodik gerecht. Die vorhersagende Polizeiarbeit auch als *Predictive Policing* tituliert — agiert mit enormen Datenfluten und verknüpft die unterschiedlichsten Ereignisse zu einem Verdachtsschema. Hier schlägt die Überwachung mit voller Kraft zu.

### Die heiße Liste

Nicht selten führen abstruse Verknüpfungen zum Verdacht. Da werden aufgrund kaum aussagekräftiger Daten aus sozialen Netzwerken bereits gefährliche Schlüsse gezogen, Jugendsünden hochstilisiert, die personellen Verbindungen im Umfeld beleuchtet. Wenn auch noch ein Kapitalverbrechen im engeren Freundeskreis geschieht, gar ein Mord, landet man zügig auf der Abschussliste — »Heat List« nennt sie die Polizei in Chicago. In den USA gibt es bereits verschiedene prädiktive Systeme.

Da werden dann aus Notrufen und Anzeigen die Wahrscheinlichkeiten für ein Verbrechen an einem bestimmten Ort zu einem bestimmten Zeitpunkt berechnet. Die »Hitzeliste« aus Illinois nimmt keinerlei Rücksicht auf die Privatsphäre. Hier werden Personendaten konkret mit einem Rating versehen, nach einem Punktesystem. Je mehr Punkte, desto näher rückt die Person in den Dunstkreis des Kriminellen. Software-Entwickler haben längst ein lukratives Geschäft erkannt. So schießen spezialisierte Firmen aus dem Boden, um das *Predictive Policing* mit effektiven Algorithmen zu unterstützen.



In Deutschland bleibt die Privatsphäre angeblich (noch) geschützt. Die Datenanalyse soll lediglich dazu beitragen, kriminelle Brennpunkte früher als bisher zu identifizieren und Beamte effektiver darauf anzusetzen.

### Geheime Techniken

Hierzulande wird die Technologie bereits in mehreren Städten genutzt — in Bonn, Hamburg, Hannover, Karlsruhe, München, Nürnberg, Stuttgart und im Ruhrgebiet. Teils sind es nur Tests; in München und Nürnberg ist das deutsche PRECOBS-System allerdings bereits seit 2016 operativ. Zu den Erfolgen gibt es bislang wenig

Konkretes und somit sehr unterschiedliche Aussagen. Die [RAND-Corporation](#) als führende US-Denkfabrik erklärt, keine merklichen Erfolge registrieren zu können. Ähnlich lautet das Ergebnis einer für die Polizeipräsidien Stuttgart und Karlsruhe durchgeführte Analyse des in Freiburg ansässigen Max-Planck-Instituts für ausländisches und internationales Strafrecht. Auch aus der Schweiz, wo Zürich, Baselland und Aargau das System testen, gibt es keine statistisch relevanten Aussagen. Oder soll die Öffentlichkeit nur beschwichtigt werden? Die Projekte befinden sich noch in den Kinderschuhen, doch schon die Grundidee gibt Anlass zur Sorge.

### **Bedrohung der Bürger nimmt zu**

Kritiker sehen im *Predictive Policing* eine Bedrohung der Unschuldsvermutung. Äußerst bedenklich auch, dass niemand einen Einblick in die Algorithmen erhält. Sie sind patentrechtlich geschützt. Das [Electronic Privacy Information Center EPIC](#) teilte am 1. November 2017 mit, einen Bericht des US-Justizministeriums über *Predictive Policing* entdeckt zu haben, den die Behörde bislang allerdings noch zurückhält. Die fadenscheinige Begründung für dieses Verhalten: Bei solchen Risikoeinschätzungen handele es sich um »*geheime Techniken*«. Und Firmen sehen ohnehin ihre Geschäftsinteressen gefährdet. Vor allem aber nimmt die Bedrohung des Bürgers zu, der uninformiert, ahnungs- und meist auch schuldlos in ein fragwürdiges System verstrickt werden kann.