«Die eigene Ungefährlichkeit kann man nicht beweisen»

6. April 2018

Timo Grossenbacher, SRF

Schweizer Polizeikorps verwenden eine Software zur Risikoprognose - diese neigt jedoch stark zur Überschätzung. Dies zeigte eine Recherche von SRF. Rechtsexperten hinterfragen die Entwicklung zur präventiven Polizeiarbeit grundsätzlich. Einer von ihnen ist Viktor Györffy, Rechtsanwalt aus Zürich und Präsident von grundrechte.ch, wo er sich für die Privatsphäre stark macht.

SRF News: Viktor Györffy, ist es neu, dass die Polizei Software zur Gefährlichkeitsprognose einsetzt, auch in der Schweiz?

Ganz neu ist es nicht - die Polizei hat ja schon immer Daten über Personen erfasst. Neu sind die Dimensionen: dass man das immer systematischer macht, diese Daten untereinander auch austauscht. Und dass man sie immer öfter computergestützt auswertet.

Vielfach redet man in diesem Zusammenhang von «Predictive Policing» - der datengetriebenen Verbrechensbekämpfung. Ist das ein Beispiel dafür?

Meiner Meinung nach schon, weil man Daten sammelt, diese analysiert und so herauszufinden versucht, ob eine bestimmte Person gefährlich ist. Gestützt auf diese Analyse wird dann allenfalls polizeilich reagiert.

Aus Sicht der Grundrechte ist das problematisch, da bei Bedrohungsanalysen notgedrungen mit vielen Vermutungen operiert werden muss. Es ist schwierig bis unmöglich, sich als Betroffener gegen solche Analysen zu wehren. Man müsste praktisch den Beweis erbringen, dass nie etwas passieren wird - und da sich solche Prognosen immer auf die Zukunft beziehen, ist das schlicht unmöglich. Computergestützte Analysen sind ohnehin schwierig zu kontern.

Wieso?

Wenn der Computer ein Ergebnis ausspuckt, erscheint das sehr genau - aber es ist pseudogenau. Will heissen: Der Computer rechnet wahrscheinlich schon korrekt und genau. Die Frage ist aber: Mit welchen Informationen füttert man ihn? Da kann das Ermessen der Behörden weit sein. Möglicherweise wird etwas eingespiesen, das schlicht falsch ist, das man aber nicht widerlegen kann. Und die Logik hinter der Berechnung kennt man ja in der Regel auch nicht.

Was meinen Sie damit?

Diese Analysetools werden in der Regel von kommerziellen Anbietern programmiert. Wie sie genau gebaut sind, bei welchen Merkmalen welche Gefährlichkeit ausgespuckt wird, kann man oft nicht nachvollziehen. Wenn das ein raffiniertes Tool mit künstlicher Intelligenz ist, wird letztlich niemand verstehen können, was da genau passiert. Das ist ja gerade der Witz: Die

Software soll einem etwas sagen, das man noch nicht weiss. Ein weiteres Problem ist die Überschätzungsgefahr...

... die ja auch bei Dyrias, der Software zur Prävention von Gewalttaten vorhanden ist, wie unsere Recherche gezeigt hat.

So ein Resultat ist immer Interpretationssache - eine genaue Vorhersage ist sowieso nicht möglich. Die Tools werden aber tendenziell so eingestellt, dass sie zu viele «Falsch Positive» ausspucken, also Personen als gefährlich einschätzen, die es gar nicht sind.

Die Polizei relativiert, die Prognoseinstrumente seien lediglich ein Puzzlestück in einer Einzelfallbewertung. Ausserdem hätten Staatsanwalt und Gerichte auch noch ein Wort mitzureden, bevor jemand sicherheitshalber verhaftet werde.

Ich denke schon, dass sich die Polizei auf die Ergebnisse dieser Tools abstützt, weil sie eben schwer zu überprüfen sind - und schwer zu widerlegen. Wenn dann der Staatsanwalt oder vielleicht ein Gericht das noch überprüfen muss, ist das Problem immer: die beschränkten Prüfungsmöglichkeiten.

Das Gericht kann ja nur hingehen und schauen, ob genügend Hinweise auf Gefährlichkeit dargelegt sind. Wenn die Polizei das Dossier dementsprechend präsentiert und die Ergebnisse des Tools hervorhebt, wird das Gericht das polizeiliche Vorgehen in der Regel absegnen. Deshalb sind solche Überprüfungen, beispielsweise durch ein Zwangsmassnahmengericht, oft nicht mehr als ein Feigenblatt.

Unsere Recherche hat auch gezeigt: Schweizweit befinden sich heute mindestens 3000 sogenannte Gefährder in polizeilichen Datenbanken. Zuerst einmal: Was ist ein Gefährder überhaupt?

Der Interpretationsspielraum ist sehr weit: Oft sind das Leute, die irgendwie gegenüber einer Behörde in Erscheinung getreten sind. Vielleicht in einer Ausnahmesituation, vielleicht in einer Auseinandersetzung - wo dann eben die Behörde die Macht hat, die Person als gefährlich zu etikettieren.

Die Erfahrung aus meiner Praxis als Rechtsanwalt zeigt: Wenn Leute einmal laut werden, heisst das noch lange nicht, dass sie auch gefährlich sind. Aber man erfasst solche Behördenkontakte je länger je systematischer. Wenn diese dann mal in solchen Informationssystemen drin sind, interpretiert man alle weiteren Begegnungen auf Basis dieser Einträge - das kann sich dann mit der Zeit verselbständigen und über Jahre so bestehen bleiben. In den allermeisten Fällen, ohne dass je einmal etwas passiert wäre.

Das erinnert fast ein bisschen an den Schweizer Fichenskandal aus den späten 80ern.

Der konkrete Hintergrund ist anders, aber eine Gemeinsamkeit gibt es: dass auf Vorrat Informationen gesammelt werden, die dann auch gegen Personen verwendet werden können - und dass diese Informationen sehr schwierig wegzukriegen sind. Anders als bei den Geheimdienst-Fichen hat man noch gewisse Rechte, insbesondere auch ein Recht, die gesammelten Daten einzusehen. Nur: Korrigieren lassen wird man sie meist nicht können.

Sie haben vorhin gesagt, die meisten Behördenkontakte würden nie gewalttätig. Nun betrifft das Bedrohungsmanagement ja aber vor allem den häuslichen Bereich, wo fast die Hälfte aller Tötungsdelikte in der Schweiz verübt werden. Ist es nicht zu begrüssen, dass die Polizei hier

genauer hinschaut?

Das ist - an sich - sicher zu begrüssen. Es stellt sich aber auch hier die Frage, ob ein solches Bedrohungsmanagement das richtige und angemessene Mittel ist. Denn es kann dazu führen, dass die Polizei völlig unterschiedlich reagiert, je nachdem, ob jemand im Computer bereits als potenziell gefährlich registriert ist oder nicht. Bei den Einen fährt die Polizei dann vielleicht schon bei geringem Anlass heftig ein.