

[Strafrecht-Strafprozessrecht](#) > [Fachbeiträge](#) > Durch Den Algorithmus Zum «gefährder»

Durch den Algorithmus zum «Gefährder»?

Monika Simmler
Giulia Canova

Einleitung

Proteste, Nötigungen und sogar Morddrohungen gegen Politiker – in Zeiten der Covid-19-Pandemie beobachtet fedpol bei Corona-Skeptikern eine steigende Gewaltbereitschaft.¹ Solche Bedrohungslagen beschäftigen die Behörden allerdings nicht erst seit Beginn der Pandemie, sondern stehen seit geraumer Zeit im Fokus der Polizeiarbeit. Ereignen sich schwere Gewalttaten und war der Täter bereits «polizeilich bekannt», werden im Nachhinein oft Vorwürfe und Forderungen nach frühzeitigen präventiven Interventionen laut. Dieser Anspruch ist Ausdruck des wachsenden gesellschaftlichen Sicherheitsbedürfnisses und widerspiegelt den Trend hin zu einer immer präventiver orientierten Sicherheitspolitik. Viele kantonale Polizeikorps institutionalisierten im Zeichen dieser Entwicklung ein umfassendes kantonales Bedrohungsmanagement («KBM»), mit welchem «Gefährder» frühzeitig erkannt und eben «gemanagt» werden sollen. Dabei setzen sie mitunter auf algorithmenbasierte Tools, welche die Behörden bei der Risikoanalyse und -prognose unterstützen. Eines dieser Tools ist das dynamische Risiko Analyse System («DyRiAS»), das bereits in mindestens sechs Kantonen zum Einsatz kommt und das Gefahrenpotenzial einzelner Personen einzuschätzen verspricht. Aber auch andere Tools wie RA-Prof («Radicalisation Profiling») oder ODARA («Ontario Domestic Assault Risk Assessment») sind in diesem Kontext gebräuchlich.² Welche Rolle derartigen Algorithmen bei der Identifikation von «Gefährdern» zukommt, was ihr Einsatz für die Betroffenen bedeutet und wie sich dabei die rechtlichen Rahmenbedingungen gestalten respektive im Rechtsstaat gestalten sollen, wird in diesem Beitrag überblicksartig diskutiert. Dabei kann auf die Erkenntnisse einer zur Lage in den Kantonen durchgeführten Studie zurückgegriffen

Gesetzesartikel

[Art. 13 Abs. 2 BV](#)
[Art. 269 StPO](#)

Rechtsgebiet(e)

Strafprozessrecht

Stichworte

[Algorithmen](#) | [Gefährder](#) | [Bedrohungsmanagement](#)

werden.³

Identifikation der «Gefährder»

Im Fokus des KBM stehen Personen, bei denen angenommen wird, dass sie in absehbarer Zeit eine Gewalttat begehen könnten und die deshalb als «Gefährder» bezeichnet werden.⁴ Das Bedrohungsmanagement kann in 3 Phasen unterteilt werden: Erkennen, Einschätzen und Entschärfen.⁵ Ins Rollen kommt dieser Prozess, sobald Behörden von äusserlich erkennbaren Warnsignalen wie Drohungen, unbefugtes Eindringen in die Wohnung der Partnerin, Stalking oder den Kauf einer Waffe Kenntnis erlangen. In einem zweiten Schritt erfolgt eine Risikoeinschätzung, wobei regelmässig Algorithmen wie DyRiAS zum Einsatz kommen. Bei der Risikobeurteilung mittels DyRiAS wird der Sachbearbeiter vom System durch einen Fragenkatalog geleitet. Im Anschluss wertet das System auf Basis eines simplen Algorithmus die Antworten aus und kalkuliert das Gefahrenpotential in Form einer Risikozahl von 1 (geringe Gefahr) bis 5 (sehr hohe Gefahr). Die DyRiAS zugrundeliegende Technik ist also wenig avanciert. Das Tool dient der Strukturierung des Beurteilungsprozesses und kann deshalb auch als spezifische Checkliste verstanden werden. Dennoch geht mit Algorithmen stets ein Verlust an Flexibilität und Individualität einher. Das Ermessen in der Risikoprognostik geht zumindest bis zu einem gewissen Grad vom Menschen auf die Technik über. Auch wenn es sich dabei nicht um eine Vollautomatisierung handelt, da die Fachperson die Ergebnisse einzuordnen hat, ist hier ein Wandel im Gange. Der Algorithmus bestimmt mit, wer ein «Gefährder» ist und wer nicht.

Einsatz des Algorithmus – objektive Analyse oder Pseudo-Legitimation?

Um die tatsächliche Rolle des Algorithmus greifbar zu machen, sind auch psychologische Komponenten zu beachten, die mit der Anwendung solcher Tools einhergehen. Der Algorithmus verspricht aufgrund seiner mathematischen Funktionsweise (vermeintlich) gleiche, gerechte und objektivere Resultate. Das Zusammenspiel zwischen Fachperson und algorithmischer Analyse kann helfen, individuelle Einschätzungen zu bekräftigen und nach aussen hin zu rechtfertigen. Der Algorithmus fungiert als «Selbstvergewisserung» und als externe Legitimationsgrundlage solange er das Bauchgefühl bestätigt. Liefert der Algorithmus hingegen ein Resultat, das dem Empfinden der Anwender zuwiderläuft, wird, wie sich in der Praxis zeigt, das konterintuitive Resultat oft hinterfragt oder gar übersteuert. In Anbetracht dieses «Bauchgefühl-Paradoxes» muss die Frage aufgeworfen werden, ob ein Algorithmus wie DyRiAS überhaupt effektiv Wirkung entfalten kann oder ob es sich dabei nicht eher um eine «Pseudo-Legitimationsgrundlage» handelt. Unabhängige Evaluationen zur Wirksamkeit dieser Tools liegen keine vor; weitere Forschung wäre dringend notwendig. Der weitgehend unkritische Algorithmeneinsatz ist deshalb fragwürdig,

insbesondere wenn auf Basis solcher Analysen tatsächlich behördlich gehandelt wird.

Bedrohungsmanagement zwischen Überwachungs- und Rechtsstaat

Mithilfe algorithmischer Risikoanalysen werden Gefährder identifiziert, die durch das KBM in der Folge speziell überwacht und betreut werden. Neben der Ergreifung proaktiver Massnahmen wie einer Gefährderansprache dient diese Betreuung dazu, die Entwicklung eines Gefährders und die von ihm ausgehende Bedrohung über längere Zeit zu überwachen. Dies bedingt zwangsläufig die Erfassung der als Gefährder klassifizierten Personen, was i.d.R. mittels «Gefährderlisten» oder vergleichbaren polizeilichen Datenbanken erfolgt. Im Jahr 2019 hatte ein mittelgrosser Kanton so z.B. bereits über 370 Gefährder auf einer Liste erfasst. Bereits die Kategorisierung einer Person in amtlichen Akten stellt einen Eingriff in die Grundrechte dar und tangiert den Schutzbereich von Art. 13 Abs. 2 BV.⁶ Die Datenbanken werden i.d.R. auch mit (besonders schützenswerten) Personendaten über den Gefährder angereichert (z.B. Beurteilung der Gewaltbereitschaft oder der psychologischen Stabilität), weshalb ein solches Datenmanagement auf jeden Fall einer expliziten gesetzlichen Grundlage bedürfte.

Da für die Kategorisierung als Gefährder weder die Begehung einer Straftat noch ein konkreter Tatverdacht verlangt wird, unterliegt das KBM der (uneinheitlichen) kantonalen Gesetzgebung, insbesondere den Polizei- und Gewaltschutzgesetzen. Liegt hingegen ein konkreter Anfangsverdacht auf eine begangene Straftat vor, kommt die StPO zur Anwendung. Ein Abstützen auf die polizeiliche Generalklausel fällt ausser Betracht, da die Funktion des KBM in der institutionalisierten Bewältigung typischer und erkennbarer Gefahrensituationen liegt. Der Erlass einer gesetzlichen Grundlage ist also unabdingbar. Nur wenige Kantone haben für das KBM allerdings Rechtsnormen geschaffen. Mit Blick auf die «Gefährderlisten», aber auch auf andere Aspekte wie die Melderechte und -pflichten, den Datenaustausch oder präventive Interventionen ist dies jedoch zwingend.⁷ Der Gesetzgebungsprozess stellte auch einen demokratischen Legitimationsprozess und den adäquaten Einbezug der Entscheidungsträger sowie der Öffentlichkeit sicher.

Bemerkenswert ist ferner der geheime Charakter vieler KBM-Massnahmen. Abgesehen von der Gefährderansprache, bei welcher der Gefährder erfährt, dass die Polizei ihm besondere Aufmerksamkeit schenkt, wird den Betroffenen ihr Status nicht mitgeteilt. Weiss der Betroffene nichts von der potentiellen Grundrechtseinschränkung, wird ihm die Überprüfung der Rechtmässigkeit verunmöglicht. Die Beobachtung des Gefährders erinnert an die geheimen Überwachungsmassnahmen nach Art. 269 ff. StPO – mit dem

gewichtigen Unterschied, dass letztere vom Zwangsmassnahmengericht genehmigt werden müssen. Es wäre daher angezeigt, auch im Bedrohungsmanagement ein Kontrollorgan einzusetzen, das die Rechtmässigkeit der Gefährderlisten und der Datenbearbeitung beaufsichtigt, während zugleich die Wirkung der Massnahmen nicht vereitelt wird.

Wie bereits dieser kurze Überblick zeigt, gilt es rund um die Gefährderthematik ein besonderes Augenmerk auf rechtsstaatliche Aspekte zu legen. Ein eigentlicher rechtswissenschaftlicher Diskurs dazu befindet sich gerade erst im Entstehen, während die polizeilichen Aktivitäten längst im Gange sind. Dass Algorithmen Bürger zu «Gefährdern» machen können ist bedenklich, dass dies ohne adäquaten rechtlichen Rahmen geschieht deutlich bedenklicher.

-
1. SRF Liveticker vom 1.11.2020, «Corona-Leugner: Drohungen gegen Behörden oder Politiker nehmen zu».
 2. Zum Einsatz dieser Tools ausführlich Monika Simmler/Simone Brunner/Kuno Schedler, «Smart Criminal Justice – Eine empirische Studie zum Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege» vom 23.11.2020.
 3. Die präsentierten Erkenntnisse basieren auf der Studie von Simmler/ Brunner/Schedler (Fn. 2), sowie dem von Monika Simmler herausgegebenen Sammelband «Smart Criminal Justice» (erscheint im Januar 2021 beim Helbing Lichtenhahn Verlag).
 4. Vgl. Karin Greuter, Erfahrungen mit dem Instrument der Gefährderansprache, in: Christian Schwarzenegger/Reinhard Brunner (Hrsg.), Bedrohungsmanagement – Häusliche Gewalt, Zürich 2018, 91, 95.
 5. Bericht des Bundesrates in Erfüllung des Postulates Feri 13.3441 vom 13.6.2013, 6 f.
 6. Oliver Diggelmann, in: Bernhard Waldmann/Eva Maria Belser/Astrid Epiney (Hrsg.), Basler Kommentar zur Bundesverfassung (BV), Basel 2015, Art. 13 N 35.
 7. Zum rechtlichen Rahmen des KBM Monika Simmler/Simone Brunner, Das Kantonale Bedrohungsmanagement: Rechtliche Grundlagen eines neuen Polizeiparadigmas, in: Monika Simmler (Hrsg.) (Fn. 2), 165 ff.

iusNet-StrafR-StrafPR 25.11.2020

Schulthess Juristische Medien AG

Schulthess §