Tobias Singelnstein

Die Sicherheit der Zukunft – Künstliche Intelligenz und soziale Kontrolle

Vom Predictive Policing zum Social Scoring[1]

Künstliche Intelligenz wird ähnliche Auswirkungen haben wie die Erfindung der Elektrizität. Mit dieser viel zitierten Feststellung hat der Informatiker und Stanford-Professor Andrew Ng die prägende Rolle künstlicher Intelligenz (KI) auf den Punkt gebracht (Armbruster, 2017). Ebenso wie die Elektrizität im 19. und 20. Jahrhundert ist auch KI eine Technologie, die in praktisch allen Lebensbereichen Einzug halten und diese mehr oder weniger grundlegend verändern wird. Die Welt der Kriminalität und der Kriminalwissenschaften macht hier keine Ausnahme. Die neuen Techniken und das ihnen zugrundeliegende Verständnis werden in den kommenden Jahrzehnten zu einem gänzlich anderen gesellschaftlichen Verständnis von Sicherheit und ihren Bedrohungen führen. Denn es ist nicht nur so, dass abweichendes Verhalten die Maßnahmen prägt, die die Gesellschaft ergreift. Aus konstruktivistischer Perspektive ist es vielmehr entgegen diesem gängigen Verständnis so, dass die Art und Weise des Umgangs mit Abweichung bestimmt, wie diese gesehen, verstanden und konzeptioniert wird.

1. Ausgangspunkte

Als Sozialkontrolle bezeichnet die Kriminologie Mechanismen, mit denen die Gesellschaft dafür sorgt, dass ihre sozialen Normen eingehalten werden. Sie unterscheidet informelle Formen im sozialen Nahraum und formelle Sozialkontrolle insbesondere durch Polizei und Strafrecht. Die Kategorie umfasst daher so unterschiedliche Dinge wie das Augenrollen unter Freund:innen einerseits und die Freiheitsstrafe andererseits. Gemein ist all diesen Mechanismen jedoch, dass sie auf dem Konzept sozialer Normen basieren und Verstöße gegen diese Normen ahnden.

Dieses rückwärtsgewandte Konzept ist in der jüngeren Vergangenheit unter Druck geraten. Es genügt der Gesellschaft nicht mehr, auf abweichendes Verhalten in der Vergangenheit zu reagieren. Vielmehr ist die vermeintliche Idealvorstellung einer umfassenden Sicherheit dominant geworden. Hierfür sollen Normverstöße präventiv verhindert werden, also schon bevor sie sich in der Praxis realisieren (Barczak, 2020; Singelnstein, 2020, S. 95, 96 ff.). Die Reaktion der Gesellschaft auf Diebstahl zum Beispiel war lange ausschließlich repressiv ausgerichtet und vor allem dem Strafrecht überlassen. Praktischer wäre es natürlich, wenn man solche Taten bereits im Vorfeld verhindern könnte. Dabei hat sich im Laufe der Zeit ein neues, instrumentelles Verständnis von Prävention und Vorsorge durchgesetzt, als für den Wohlfahrtsstaat der alten Bundesrepublik prägend war – von Gefahrenabwehr und Strafverfolgung über Prävention hin zu Prädiktion und Präemption (Volkmann, 2021, S. 1408, 1409 ff.). Es geht nicht um die Veränderungen von sozialen Bedingungen und Lebenslagen im Sinne primärer Prävention, sondern um die konkrete Intervention bei Situationen und Personen, denen Risiken zugeschrieben werden (Singelnstein & Kunz, 2021, S. 391 ff.). Zentrale Voraussetzung für diese Vorstellung

[1] Es handelt sich um die aktualisierte Version des Beitrages, der erstmals veröffentlicht wurde in Horst Beisel u. a. (Hrsg.), Die Kriminalwissenschaften als Teil der Humanwissenschaften. Festschrift für Dieter Dölling zum 70. Geburtstag, Baden-Baden 2023, 963 ff.

ist, dass man schadensträchtige Situationen und potenziell gefährliche Personen identifizieren kann, bevor der Schaden eingetreten ist (allgemein zur Wissensproduktion im Sicherheitsrecht Rusteberg, 2019, S. 233). Neue Formen sozialer Kontrolle arbeiten hierfür mit dem Konzept des Risikos. Hierunter versteht man kurz gesagt ein wahrgenommenes Schadenspotential. Es geht also um Umstände, die statistisch betrachtet das Auftreten eines Schadens oder abweichenden Verhaltens wahrscheinlicher machen. Zum Beispiel weist man als junger Mensch eine höhere Wahrscheinlichkeit auf, Straftaten zu begehen, als im fortgeschrittenen Alter.

Künstliche Intelligenz ist ein schillernder Begriff. Er umfasst sehr verschiedene Techniken, wie zum Beispiel Machine Learning, Robotik und neuronale Netze. Künstliche Intelligenz hat also viele Gesichter und wird schon heute in ganz unterschiedlichen Bereichen angewendet, wie Übersetzungsdiensten im Internet, Deepfake-Apps zur Manipulation von Videos, autonomem Fahren, Drohnen oder Waffensystemen. Allerdings handelt es sich bei alldem noch um recht simple Formen, man könnte auch sagen Vorformen von künstlicher Intelligenz im eigentlichen Sinne, deren Zusammenspiel mit der realen Welt häufig nur ungenügend funktioniert. Es gibt Maschinen, die bestimmte Muster ausführen, auf die sie programmiert wurden, wie etwa Roboter in der Industrie. Programme und Algorithmen können mit großen Mengen von Daten trainiert werden, um bestimmte Muster zu erkennen, wie etwa beim autonomen Fahren. Aber wir sind noch sehr weit entfernt von Maschinen, die tatsächlich wie Menschen agieren, die tasten und greifen können, die es schaffen, ihnen unbekannte Situationen angemessen zu bewältigen (Niederée & Nejdl, 2020, S. 42).

2. Künstliche Intelligenz und soziale Kontrolle

Für die Kriminalwissenschaften bedeuten die beschriebenen technischen Entwicklungen einerseits neue Herausforderungen und Probleme. Ganz generell stellt sich bei derart automatisierten Prozessen die Frage, wie negative Folgen zugerechnet werden können (s. z.B. Lohmann, 2021). Wer ist verantwortlich, wenn beispielsweise eine autonom fliegende Drohne einen Unfall verursacht? Ebenso sorgen die neuen Techniken für neue Formen von Kriminalität. Hier stellt sich die Frage, ob diese unter bereits bestehende Straftatbestände gefasst werden können oder ob neue Normen erforderlich sind.

Die KI eröffnet aber auch neue Chancen für soziale Kontrolle (Übersicht bei Baur, 2020, S. 275; Rademacher, 2021, S. 229, 234 ff.). Sie wird etwa eingesetzt, um schon bestehende Aufgaben zu erleichtern: In den USA gibt es etwa das Predictive Sentencing, das Richter:innen bei ihren Entscheidungen berät, und auch in Deutschland hält die Automatisierung in der Rechtspflege Einzug (Eisbach et al., 2022, S. 489; Fries, 2018, S. 414; Kaspar et al., 2020, S. 35; Kessler, 2020, S. 605; Ofterdinger, 2020, S. 404). Die Polizei in Deutschland entwickelt Tools, um Handschriften abzugleichen und zu identifizieren oder sexuellen Missbrauch von Kindern auf Bildern zu erkennen (Landeskriminalamt Niedersachsen, 2024, S. 18 f.); Algorithmen sollen musterbasiert Geldwäsche, Steuerhinterziehung oder andere Wirtschaftsstraftaten erkennen; Uploadfilter von privaten Unternehmen auf digitalen Plattformen erkennen abweichendes Verhalten und schließen es aus; Videoüberwachung kann Personen identifizieren – nicht nur im Wege der Gesichtserkennung, sondern zukünftig bspw. auch an der Art ihres Ganges.

KI ist aber nicht nur Hilfswerkzeug. Sie ermöglicht ebenso vollkommen neue Formen sozialer Kontrolle. Durch die Analyse von Mustern und Zusammenhängen in Kriminalitätsdaten soll es möglich werden, abweichendes Verhalten vorherzusagen. Intelligente Videoüberwachung kann Verhaltensweisen erkennen, die für gefährliches oder strafbares Verhalten typisch sind, wie etwa hektische Bewegungen mehrerer Personen an einem gefährlichen Ort (Golla, 2020, S. 149, 156 f.). Perspektivisch soll sie auch Gesichtsausdrücke interpretieren können, um daraus Motivationen und Haltungen wie zum Beispiel Kaufinteressen, sexuelles Interesse oder Suizidabsichten zu lesen, oder in der Lage sein, Corona-Infektionen zu erkennen (Behr, 2021). Predictive Policing – also die Vorhersage von Straftaten durch Massendatenauswertung – steckt in Deutschland zwar noch in den Kinderschuhen. Ein Blick in die USA zeigt jedoch, wie sehr das Konzept zukünftig die Polizeiarbeit bestimmen wird (Singelnstein, 2018, S. 1, 2 ff.).

Diese neuen Techniken unterstützen damit nicht bereits bestehende Formen sozialer Kontrolle, wie etwa das Strafrecht. Sie treten als gänzlich neue Formen vielmehr an deren Stelle und zeichnen sich dabei durch zwei Merkmale aus. Erstens folgen sie einer probabilistischen Perspektive, treffen also Wahrscheinlichkeitsaussagen unabhängig von einem konkreten Anlass und weit im Vorfeld möglicher Schädigungen. Dies kann sowohl personenbezogen als auch situationsbezogen erfolgen. Zweitens favorisieren sie eine Bearbeitung schon dieser Risiken im Vorfeld, die wiederum verschiedener Art sein kann. Zum einen kann sie in einer genaueren Untersuchung der Lage oder einer entsprechenden Informationsbeschaffung bestehen. Zum anderen kann aber auch eine unmittelbare Intervention in das jeweilige Geschehen vorgenommen werden, um eine Veränderung für die Zukunft zu erreichen, was als Präemption bezeichnet wird (Egbert, 2018, S. 106, 109 ff.). Damit behaupten diese Techniken, den lang gehegten Wunsch sozialer Kontrolle – nämlich Abweichung präventiv zu verhindern – Wirklichkeit werden zu lassen. Im Fall des Diebstahls müsste man die Tat also nicht mehr abwarten. Man könnte vielmehr anhand des Gesichtsausdrucks oder sonstiger sozialer Merkmale potentieller Täter:innen erkennen, ob bei ihnen eine erhöhte Wahrscheinlichkeit besteht, einen Diebstahl zu begehen.

3. Problemstellen und Fragezeichen

Der Umgang mit Risiken, wie ihn solche neuen Techniken sozialer Kontrolle praktizieren, lässt sich abstrakt betrachtet in drei Schritte unterscheiden: Berechnung bzw. Identifizierung, Bewertung und Management.

3.1. Risikoidentifizierung

Auf der Ebene der Risiko-Identifizierung oder -Berechnung gilt es, Faktoren zu ermitteln, die das Auftreten abweichenden Verhaltens für bestimmte Personen oder Situation wahrscheinlicher machen (Singelnstein & Kunz, 2021, S. 394 ff.). Die Systeme arbeiten dafür nach dem Prinzip der Mustererkennung. In einem ersten Schritt werden hierfür sehr große Datenbestände daraufhin untersucht, ob sich bestimmte Muster identifizieren lassen, die mit abweichendem Verhalten in Verbindung stehen. Das können sehr verschiedene Sachen sein. Zum einen ganz konkrete Dinge, wie ein bestimmtes Verhalten oder ein bestimmter Gesichtsausdruck im Fall der intelligenten Videoüberwachung. Zum anderen gibt es aber auch umfassende

Vorgehensweisen wie im Fall von Predictive Policing-Systemen, die anhand sehr vieler verschiedener Daten Profile von Personen erstellen oder Situationen analysieren. Sind Muster erkannt, die statistisch betrachtet die Begehung von Straftaten wahrscheinlicher machen, werden die Systeme darauf trainiert, diese in der realen Welt zu erkennen, um sie dort bewerten und managen zu können (Kaufmann et al., 2019, S. 674).

Auf diese Weise eröffnet KI durchaus interessante neue Perspektiven. Unter Umständen kann sie sogar Einsichten ermöglichen, die uns bisher verborgen waren, denn menschliches Verhalten ist in gewissem Umfang durchaus messbar und berechenbar. Sie führt auf diese Weise zu einem veränderten Verständnis von Risiko (Hannah-Moffat, 2019, S. 453). Allerdings ist die Risikoidentifizierung im Bereich sozialer Kontrolle abweichenden Verhaltens auch mit grundlegenden Schwierigkeiten verbunden, insbesondere mit Nichtwissen über Risiken, das einer sauberen Definition von Mustern entgegensteht. Erstens ist menschliches Verhalten nur in mancher Hinsicht messbar und berechenbar; gibt es in unterschiedlichem Maße Muster, sind manche Risikofaktoren besser zu prognostizieren als andere. Zweitens hängt die Qualität der Mustererkennung stark von der Komplexität des jeweiligen Gegenstandes ab.

Schließlich braucht es für diese Prozesse Erhebungen und Verarbeitungen (auch) personenbezogener Daten in ganz erheblichem Umfang (Egbert, 2020, S. 77). Zum einen sind große Datenbestände erforderlich, mit denen die Techniken trainieren und arbeiten können, um zum Beispiel Muster zu erkennen – je mehr und je unterschiedlichere Daten, umso besser. Zum anderen müssen diese Techniken, wenn sie dann funktionieren, permanent uns und unsere Welt vermessen, um Muster und Risikofaktoren entdecken zu können (Kuhlmann & Trute, 2021, S. 103, 108 f.; s. auch Golla, 2020, S. 149, 157 f.). Je umfassender diese vorsorgende Überwachung ist, sei es durch Videoüberwachung oder durch Datenauswertungen, desto mehr können die Techniken entdecken.

Wegen des Eingriffscharakters solcher Maßnahmen im Hinblick auf die informationelle Selbstbestimmung dominieren in Deutschland bislang Ansätze, die auf Situationen schauen und daher keine personenbezogenen Daten verarbeiten. Zunehmend betreten aber auch Formen der personenbezogenen Risikoanalyse die Bühne (Sommerer, 2020). Diese konzentrieren sich derzeit noch auf bestimmte Gruppen, wie Intensivtäter:innen, Sexualstraftäter:innen und Gefährder:innen, arbeiten dabei vor allem mit schon bestehenden polizeilichen Datenbeständen und setzen noch keine KI ein, wie die polizeilichen Datenbanken, aber etwa auch das Programm RADAR (Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos) des BKA zeigen (dazu Sonka et al., 2020, S. 386). Verschiedene Projekte vor allem aus dem Sicherheitsforschungsprogramm des BMBF zeigen aber, wohin die Reise gehen soll: datenbasierte, möglichst automatisierte Risikoanalysen auch bezüglich Personen. Dabei kann auf sehr unterschiedliche Datenbestände zurückgegriffen werden, unter anderem auch solche aus sozialen Medien (Spranger & Labudde, 2020, S. 653.).

3.2. Risikobewertung

Deutlich schwieriger wird das Ganze, wenn es um die Bewertung der jeweiligen Risiken geht, also um die Frage, was das Vorliegen eines Risikofaktors eigentlich konkret bedeutet und was daraus folgen soll. Hier haben die neuen Techniken sozialer Kontrolle wie alle Formen der

Prognose mit den Problemen Ambivalenz, Komplexität und Unsicherheit zu kämpfen. Diese zeigen sich bei der Prognose abweichenden Verhaltens in ganz besonderem Maße. Denn dieses ist nicht nur höchst vielfältig, sondern es handelt sich auch um sozial sehr komplexe Geschehen, die von einer Vielzahl sehr unterschiedlicher Faktoren beeinflusst sein können.

Ob und warum jemand gegen soziale Normen verstößt, ist von unzähligen Faktoren abhängig, die sehr langfristig wirken, aber ebenso auch von spontanem Einfluss sein können. Zwar gibt es mittlerweile eine Vielzahl kriminologischer Theorien, die die Entstehung von Kriminalität auf die eine oder andere Weise erklären. Je nach Epoche und gültigem Paradigma suchen sie die Ursachen von Abweichung dabei in Anlage oder Umwelt, in biologischen, psychologischen, sozialen oder sozialstrukturellen Umständen. Aber: Wir kennen eigentlich nur einzelne Faktoren, die das Auftreten abweichenden Verhaltens wahrscheinlicher machen. Es gibt keine Weltformel für die Erklärung von Kriminalität (Singelnstein & Kunz, 2021, S. 219 ff.). Und die theoretische und empirische Klärung von Entstehungszusammenhängen von Kriminalität ist eine Sache. Etwas völlig anderes ist die konkrete Vorhersage abweichenden Verhaltens bestimmter Personen. Selbst im Bereich der Kriminalprognosen, die eine sehr spezifische Population von Proband:innen bzw. sehr spezifische Fragestellungen betreffen, sind die methodischen Möglichkeiten, zukünftige Straffälligkeit zu prognostizieren, hoch umstritten und alles andere als zufriedenstellend (s. nur Eisenberg & Kölbel, 2024, S. 192 ff.).

Wer aber einmal als risikohaft, als Gefährder:in erfasst ist, der:die hat es schwer, sich zu exkulpieren, sich von diesem Label zu befreien. Wo nichts Konkretes vorgeworfen wird, sondern nur eine vage Einschätzung besteht, kann man sich nicht überzeugend entlasten. Welche kafkaesken Züge das annehmen kann, haben die europäischen und internationalen Flugverbotslisten eindrucksvoll vor Augen geführt (Biermann & Wolfangel, 2023).

3.3. Risikomanagement

Im dritten Schritt stellt sich sodann die Frage, wie mit den identifizierten und bewerteten Risiken umgegangen wird. Hier gibt es verschiedene mögliche Formen. Zum einen gibt es sogenannte Recommender-Systeme. Diese geben Informationen und Empfehlungen, wie eine bestimmte Situation zu behandeln ist, entscheiden aber nicht selbst. Hierzu zählen etwa Predictive Sentencing-Systeme, die Richter:innen bei der Entscheidungsfindung unterstützen sollen (Rühl, 2022, S. 272 ff.). Für solche Systeme stellt sich stets die Frage, inwieweit die Entscheider:innen daneben selbst zu einer qualifizierten Beurteilung in der Lage und fähig sind, den Empfehlungen ggf. auch zu widerstehen. Zum anderen sind auch Systeme mit automatisierten Entscheidungen möglich, etwa wenn ein System intelligenter Videoüberwachung Alarm auslöst oder Räume abriegelt.

Auch inhaltlich lassen sich verschiedene Möglichkeiten des Managements von Risiken denken. Erstens kommt eine konkrete Steuerung in Betracht, also eine Intervention, um eine bestimmte Risikosituation zu bearbeiten. Diese Bearbeitung könnte etwa in der Risikoerforschung bestehen, indem zum Beispiel Polizist:innen zu einem bestimmten Ort beordert werden, wo die Wahrscheinlichkeit von Einbrüchen gesteigert sein soll, oder wenn potentiell gefährliche Personen beobachtet werden, um weitere Informationen über sie und ihr Tun zu beschaffen, um zu klären, ob sich eine Gefahr konkretisiert (Sprenger, 2020, S. 967 ff.). Ebenso kommt aber auch

eine unmittelbare Gestaltung der Risikosituation in Betracht. Einem potentiellen Dieb könnte beispielsweise der Zugang zum Kaufhaus verwehrt werden, wenn die Videoüberwachung bei ihm einen entsprechend verdächtigen Gesichtsausdruck identifiziert.

Zweitens gibt es Vorsorgemodelle, die an allgemeinere Risikovorhersagen mehr oder weniger umfassende Konsequenzen knüpfen. Hier geht es also nicht darum, konkrete identifizierte Risiken gezielt zu bearbeiten, wie eine erhöhte Einbruchs- oder Diebstahlswahrscheinlichkeit. Stattdessen wird anhand einer Vielzahl von Parametern die generelle Risikohaftigkeit von Personen in Form von Risikoprofilen bestimmt, um daran dann ein ebenso breites Feld an Reaktionen im Sinne der Vorsorge zu knüpfen. Wie das in der Praxis aussehen kann, das zeigt ein Blick nach China mit seinem berüchtigten Social Scoring System (Kühnreich, 2020, S. 209) – oder in die Privatwirtschaft. Auch in Deutschland setzen die SCHUFA oder Versicherungen das sogenannte Social Scoring längst ein, um die Kreditwürdigkeit oder die Wahrscheinlichkeit von Versicherungsfällen einzuschätzen (s. hierzu Maamar, 2018, S. 820 ff.). Im Falle der SCHUFA kann diese Form des Risikomanagements dazu führen, dass man keine oder nur sehr teure Kredite bekommt oder bestimmte Verträge nicht mehr abschließen kann. Das chinesische Social Scoring System schließt ab einem bestimmten Punktwert Personen zum Beispiel davon aus, Tickets für Flüge und Bahnfahrten zu kaufen. Auf diese Weise wird einem erhöhten, nicht notwendig weiter spezifizierten Risikoprofil begegnet, bevor sich diese Risiken weiter konkretisieren.

Zugleich sind solche Formen des vorsorgenden Ausschlusses aber natürlich auch Sanktionen und damit Anreiz zum Wohlverhalten, zur Selbstführung. Ein solcher Anreiz muss aber nicht unbedingt derart offen daherkommen, sondern kann auch im Gewand der Manipulation agieren. KI und Algorithmen bieten hierfür hervorragende Möglichkeiten, denn sie kennen uns zunehmend besser, können nicht nur Verhalten und Entscheidungen vorhersagen, sondern wissen auch um unsere Bedürfnisse, Wünsche und Ängste (Zeit Online, 2019). Technisch besehen ist der Schritt zum Risikomanagement durch Manipulation dann nicht mehr allzu groß.

Wir sehen also durchaus unterschiedliche Techniken – das diesen zugrunde liegende Prinzip ist jedoch das gleiche, nämlich Risikomanagement. Letztlich erscheint staatliches Social Scoring aus dieser Perspektive nur als konsequente Weiterentwicklung der auch heute schon in Deutschland eingesetzten Techniken.

4. Die Sicherheit der Zukunft

Die beschriebenen Techniken und Strategien im Kontext KI werden zu einem grundlegend anderen Bild von abweichendem Verhalten und Kriminalität führen – und auf diese Weise ein grundlegend anderes gesellschaftliches Verständnis von Sicherheit herstellen. Sicherheit ist ein soziales Konstrukt. Dessen Form und Veränderung ist von den jeweiligen gesellschaftlichen Bedingungen und den bestehenden gesellschaftlichen Diskursen geprägt. Wie viel Sicherheit ist notwendig? In welchen Bereichen und Themenfeldern? Wessen Sicht ist dabei maßgeblich? Was bedeutet Sicherheit genau – also wann liegt sie vor und wann ist sie gestört? Diese Fragen werden zu unterschiedlichen Zeiten und in unterschiedlichen Gesellschaften, aber auch von unterschiedlichen Gruppen in der Gesellschaft verschieden beantwortet. Zentral hierfür ist, was

eine Gesellschaft unter Störungen und Bedrohungen versteht, was also Quellen der Verunsicherung sind und welche Konzepte für einen Umgang damit favorisiert werden.

4.1. Störungen der Sicherheit der Zukunft

Als Störungen der Sicherheit, als Quellen von Verunsicherung und Bedrohung werden zukünftig ganz andere Dinge verstanden werden als heute. Im Zentrum stehen nicht mehr Kriminalität und das von sozialen Normen abweichende Verhalten, wie sie heute durch das Strafrecht und verwandte Techniken sozialer Kontrolle hervorgebracht werden. Stattdessen werden bereits Risikofaktoren, wie sie von den neuen KI-Techniken sozialer Kontrolle thematisiert und bearbeitet werden, als Störungen der Sicherheit angesehen werden (Hannah-Moffat, 2019, S. 453).

Normal ist danach nicht, wer lediglich verbotenes Verhalten unterlässt. Normal ist, wer keine Risikofaktoren für zukünftiges abweichendes Verhalten aufweist. In der Welt der probabilistischen Sichtweisen wird die Berechenbarkeit von Risiken zur entscheidenden Frage. Diese Techniken – und damit wir – werden nicht mehr danach schauen, ob Handlungen von Menschen Normen verletzen, was eine sehr exakte Feststellung erfordert. Stattdessen berechnen sie Wahrscheinlichkeiten einer möglichen Normverletzung in der Zukunft und betrachten bereits diesen Risikofaktor weit im Vorfeld einer Schädigung als Störung. Diese Perspektive führt dazu, dass wir nicht mehr auf einzelne Handlungen von Menschen schauen und diese bewerten, wie wir es bislang im Strafrecht tun. Vielmehr nehmen wir Personen und Situationen als solche in den Blick und unterziehen sie bei der Risikoanalyse einer vorausschauenden Gesamtbewertung. Bei Personen eröffnet dies die Möglichkeit, ein Rating vorzunehmen, die Bevölkerung also in verschiedene Risikoklassen einzuteilen. Denken wir zurück an das Beispiel des Diebstahls: Ein Dieb gerät dann nicht erst ins Blickfeld, wenn er den Diebstahl begeht, sondern bereits, wenn er mit einem verdächtigen Gesichtsausdruck das Kaufhaus betritt oder ansonsten Risikomerkmale aufweist, die für eine Begehung von Diebstählen sprechen – junges Alter, falsche Wohngegend, Vorbelastung. Das mag bei einer Person, die tatsächlich einen Diebstahl begehen will, praktisch sein. Es trifft aber auch Dutzende andere, die zwar ähnliche Risikomerkmale aufweisen, tatsächlich aber keinen Diebstahl begehen würden. Die Techniken beurteilen eben nicht Individuen als solche, sondern konstruieren Gruppen anhand von Wahrscheinlichkeitsaussagen.

Durch das veränderte Verständnis von Störungen der Sicherheit werden ganz andere Phänomene ins Zentrum der Betrachtung rücken. Welche Formen von Störungen im Zentrum der gesellschaftlichen Wahrnehmung stehen und wie sie verstanden werden, hängt immer auch von den jeweiligen Strategien ab, mit denen eine Gesellschaft sich um die Kontrolle dieser Störungen bemüht. So wurden Wiederholungstäter:innen erst zum Gegenstand, als es durch polizeiliche Karteien und Spurensicherung möglich wurde, einzelnen Verdächtigen mehrere Straftaten nachzuweisen. Dort wo Prognosen wie bei der KI anhand von Mustererkennung vorgenommen werden, rücken naturgemäß solche Störungen in den Fokus, die bestimmte Muster aufweisen. Und die gesellschaftliche Wahrnehmung wird sich stärker auf äußere Anzeichen solcher Muster denn auf Einstellungen, soziale Erklärungen und ähnliche Entstehungszusammenhänge konzentrieren (Singelnstein, 2018, S. 1, 4 f.). In der Kriminologie werden andere Kriminalitätstheorien stärker werden, die dieser musterbasierten, äußeren Perspektive folgen.

Dieser grundlegende Wandel führt indes nicht dazu – wie man vielleicht hoffen könnte –, dass es keine Störungen der Sicherheit mehr geben würde. Vielmehr ändert sich nur das Verständnis dessen, was als Störung anzusehen ist – nämlich bereits der Risikofaktor weit im Vorfeld einer tatsächlichen Schädigung oder Rechtsgutsverletzung.

4.2. Umgang mit Störungen der Sicherheit der Zukunft

Der Umgang mit Störungen von Sicherheit – also die Berechnung und Bewertung und das Management von Risiken – liegt zu einem erheblichen Teil in staatlicher Hand und ist Aufgabe vor allem der Polizei. Zugleich prägt das neue Verständnis aber auch die Praxis der Bürger:innen. Sie sind im Alltag bemüht, Risiken zu erkennen und ihnen vorsorgend zu begegnen. Präventionsprogramme der Polizei halten sie sogar dazu an. Schutz vor Bedrohungen und Sorge für Sicherheit ist also heute mehr als in vergangenen Jahrzehnten auch ein Projekt des Einzelnen. Schließlich wird die Herstellung von Sicherheit zunehmend zu einem Markt. Private Unternehmen bieten eigene Lösungen zur Risikoberechnung und -bewertung sowie entsprechende Vorsorgemaßnahmen an. Sie regen damit sowohl das staatliche als auch das private Risikomanagement weiter an (Ulbricht & Egbert, 2024, S. 1 ff.).

Welches Ausmaß dieses Risikomanagement in der Gesellschaft annehmen wird, ist von heute aus betrachtet schwer zu sagen. Denkbar wäre etwa das Management von lediglich besonders erheblichen Risiken. Ließen sich etwa hinreichend konkrete Muster und Risikofaktoren für Tötungsdelikte ermitteln, könnte man diesen mit einer punktuellen Steuerung durch Maßnahmen der Risikoerforschung begegnen. Am anderen Ende der Skala steht das Modell eines umfassenden Risikomanagements, wie es in China favorisiert wird: Durch die umfassende Vermessung der Welt, der Menschen und ihrer Handlungen durch intelligente Videoüberwachung und vielfältige Datenauswertungen findet eine permanente Berechnung von Risiken statt, die im Wege der schon allgegenwärtigen Gesichtserkennung Personen zugeordnet werden können (Genzsch, 2019, S. 129, 136 ff.; Behr, 2021). Identifizierung und Risikodetektion als verschiedene Anwendungsfelder von KI sind hier also miteinander verbunden. Das erforderliche Management wird im Vorsorgemodell in Form eines Sozialkredit-Systems umgesetzt.

In welche Richtung die Entwicklung in Deutschland und Europa geht, wird stark davon abhängen, ob der Gesellschaft ein rationaler Umgang mit einschlägigen Risikofaktoren gelingt. Schließlich ist es gerade deren Merkmal, dass sie nur Wahrscheinlichkeitsaussagen treffen und sich nicht in jedem Fall realisieren. Allerdings gibt es – was das angeht – wenig Anlass für Optimismus. Dies zeigt nicht alleine unser heutiger Umgang mit Sicherheitsstörungen und Kriminalität, der oft wenig rational und evidenzbasiert daherkommt. Auch nach den Befunden der Risikoakzeptanzforschung wird unserer Gesellschaft ein rationaler Umgang äußerst schwerfallen. Diese Risiken bringen nämlich praktisch alles mit, was sie besonders wenig akzeptabel macht: Sie werden nicht freiwillig eingegangen, sondern sind aufgedrängt; sie sind schlecht kontrollierbar und meist ohne positiven Nutzen, dafür unter Umständen mit schweren Folgen verbunden und betreffen potentiell alle oder viele Menschen (Zwick, 2020, S. 29, 40 ff.). Und der damit verbundene Anspruch der Prävention ist schier endlos, nie ausreichend, kann immer noch weitergehen, ist immer noch früher möglich und findet stets noch weitere Risikofaktoren.

5. Schluss

Die Techniken künstlicher Intelligenz bringen für den Bereich sozialer Kontrolle neue Möglichkeiten und die Chance auf innovative Einsichten. Sie versprechen praktisch genau das, was bislang nicht möglich war. Gleichzeitig bergen sie aber auch massive Probleme und werfen grundlegende Fragen auf. Erstens können wir Risiken für abweichendes Verhalten in der Zukunft – jedenfalls von heute aus betrachtet – nur sehr unzureichend berechnen und bewerten. Solche Techniken werden daher vor allem bestehende Kriminalitätsbilder mit all ihren Verzerrungen reproduzieren (Wehrheim, 2014, S. 137). Wo liegen ethische Grenzen für eine solche KI? Wie können effektive Kontrolle und rechtliche Regulierung solcher Algorithmen organisiert werden? Ist die Berechnung, die Vermessung dem Zufall tatsächlich überlegen?

Zweitens fungiert KI auf diese Weise als Motor für einen grundlegenden Wandel sozialer Kontrolle. Diese setzt heute zunehmend auf das Management von Risiken, um mögliche Schädigungen bereits im Vorfeld zu verhindern. Dies zusammengenommen formt die Sicherheit der Zukunft, also unser Bild von Sicherheit, Störungen und Unsicherheit und wie die Gesellschaft damit umgehen sollte. Sicherheit in diesem Sinne wird immer wichtiger. Sie wird zunehmend als Ideal einer absoluten Sicherheit formuliert. Und sie erscheint als eine Sicherheit, die angesichts von Risiken ständig bedroht ist – was subjektiv betrachtet wiederum eher für Verunsicherung als für Sicherheit sorgt, sodass ein permanenter Loop entsteht. Wo sind die Grenzen einer solchen Entwicklung, einer derart steten Vorverlagerung?

Drittens schließlich ist der beschriebene Wandel, sind die Strategien des Risikomanagements mit äußerst problematischen Konsequenzen verbunden, namentlich mit chilling effects (dazu Moll & Schneider, 2021, S. 92): Je umfassender Risikoerkennung und Risikomanagement als Formen sozialer Kontrolle ausgestaltet sind, umso höher ist der Druck für den Einzelnen, sich konform zu verhalten, nicht aufzufallen. Diese sanfte Einschränkung von Autonomie und Freiheit, die ohne Zwang auskommt, mag einerseits effizient sein. Sie ist andererseits aber auch gefährlich, gerade weil sie weniger auffällt und sich der gesellschaftlichen Auseinandersetzung entzieht. Wo sind im demokratischen Rechtsstaat absolute Grenzen für diese Formen der Beeinflussung und Manipulation? Inwieweit ist unsere zeitgenössische Dogmatik, ist insbesondere das Verfassungsrecht geeignet, diese Grenzen in der Praxis zu bewahren – gerade angesichts des machtvollen Bildes von der Sicherheit der Zukunft, das sich herauszubilden beginnt?

Literatur

Armbruster, A. (2017, 22. März). Er ist ein Star der künstlichen Intelligenz. *Frankfurter Allgemeine Zeitung.* **https://www.faz.net/aktuell/wirtschaft/netzwirtschaft/andrew-ng-er-ist-ein-star-der-kuenstlichen-intelligenz-14936979.html**. Zugegriffen: 18.2.2022.

Barczak, T. (2020). *Der nervöse Staat: Ausnahmezustand und Resilienz des Rechts in der Sicherheitsgesellschaft.* Mohr Siebeck.

Baur, A. (2020). Maschinen führen die Aufsicht. Offene Fragen der Kriminalprävention durch digitale Überwachungsagenten. *Zeitschrift für Internationale Strafrechtsdogmatik, 15*(6), 275-284.

Behr, W. (2021, 18. April). Gesichtsverlust 3.0. *geschichte der gegenwart.* **https://geschichtedergegenwart.ch/gesichtsverlust-3-0/**. Zugegriffen: 18.02.2022.

Biermann, K., & Wolfangel, E. (2023, 13. Februar). No-Fly-List der USA: In schlechter Gesellschaft. *Zeit Online.* **https://www.zeit.de/politik/2023-02/usa-no-fly-liste-einreise-terrorismus-unschuld/komplettansicht**. Zugegriffen: 21.01.2025.

Egbert, S. (2018). Drogentests und 'Alltags-Präemption'. *Kriminologisches Journal, 50*(2), 106-122.

Egbert, S. (2020). Datafizierte Polizeiarbeit – (Wissens-)Praktische Implikationen und rechtliche Herausforderungen. In D. Hunold & A. Ruch (Hrsg.), *Polizeiarbeit zwischen Praxishandeln und Rechtsordnung* (S. 77-100). Springer.

Eisbach, S., Heghmanns, M., & Hertel, G. (2022). Künstliche Intelligenz im Strafverfahren am Beispiel von Kriminalprognosen. *Zeitschrift für Internationale Strafrechtswissenschaft 1*(7-8), 489-496.

Eisenberg, U., & Kölbel, R. (2024). *Kriminologie, 8. Aufl*. Mohr Siebeck.

Fries, M. (2018). Automatische Rechtspflege. *Rechtswissenschaft, 9*(4), 414-430.

Golla, S. (2020). Lernfähige Systeme, lernfähiges Polizeirecht. Regulierung von künstlicher Intelligenz am Beispiel von Videoüberwachung und Datenabgleich. *Kriminologisches Journal, 52*(2), 149-162.

Genzsch, M. (2019). Harmonie durch Kontrolle? Chinas Sozialkreditsystem. In T. Loitsch (Hrsg.), *China im Blickpunkt des 21. Jahrhunderts* (S. 129-142). Springer.

Hannah-Moffat, K. (2019). Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates. *Theoretical criminology, 23*(4), 453-470.

Kaspar, J., Höffler, K., & Harrendorf, S. (2020). Datenbanken, Online-Votings und künstliche Intelligenz – Perspektiven evidenzbasierter Strafzumessung im Zeitalter von „Legal Tech“. *Neue Kriminalpolitik, 32*(1), 35-56.

Kaufmann, M., Egbert, S., & Leese, M. (2019). Predictive Policing and the Politics of Patterns. *The British Journal of Criminology*, *59*(3), 674-692.

Kessler, C. (2020). KI und Legal Tech. Utopie, Dystopie, Realität. In S. Beck, C. Kusche & B. Valerius (Hrsg.), *Digitalisierung, Automatisierung, KI und Recht* (S. 607-628). Nomos.

Kuhlmann, H.-H., & Trute, S. (2021). Predictive Policing als Formen polizeilicher Wissensgenerierung. *Zeitschrift für das Gesamte Sicherheitsrecht, 5*(3), 103-111.

Kühnreich, K. (2020). Social Credit, Sicherheit und Freiheit. In O. Everling (Hrsg.), *Social Credit Rating* (S. 209-226). Springer.

Landeskriminalamt Niedersachsen (Hrsg.) (2024). *Cybercrime und Kinderpornographie in Niedersachsen. Lagebild.*

Lohmann, A. (2021). *Strafrecht im Zeitalter von Künstlicher Intelligenz. Der Einfluss von autonomen Systemen und KI auf die tradierten strafrechtlichen Verantwortungsstrukturen*. Nomos.

Maamar, N. (2018). Social Scoring. Eine europäische Perspektive auf Verbraucher-Scores zwischen Big Data und Big Brother. *Computer und Recht, 34*(12), 820-828.

Moll, R., & Schneider, F. (2021). Ausbau der Datenerhebungsbefugnisse von Sicherheitsbehörden – Lässt die wissenschaftliche Empirie Chilling-Effekte in der Bevölkerung erwarten? *Monatsschrift für Kriminologie und Strafrechtsreform*, *104*(2), 92-106.

Niederée, C., & Nejdl, W. (2020). Technische Grundlagen der KI. In M. Ebers, C. Heinze, T. Krügel & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik. Rechtshandbuch* (S. 42-74). C.H.Beck.

Ofterdinger, H. (2020). Strafzumessung durch Algorithmen? *Zeitschrift für Internationale Strafrechtsdogmatik, 15*(9), 404-410.

Rusteberg, B. (2019). Wissensgenerierung in der personenbezogenen Prävention – Zwischen kriminalistischer Erfahrung und erkenntnistheoretischer Rationalität. In L. Münkler (Hrsg.), *Dimensionen des Wissens im Recht* (S. 233-265). Mohr Siebeck.

Rademacher, T. (2021). Verdachtsgewinnung durch Algorithmen. Maßstäbe für den Einsatz von predictive policing und retrospective policing bei Gefahrenabwehr bzw. Strafverfolgung. In D. Zimmer (Hrsg.), *Regulierung für Algorithmen und Künstliche Intelligenz* (S. 229-268). Nomos.

Rühl, G. (2022). Einsatz von KI-Systemen in der Justiz. In Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz & F. Rostalki (Hrsg.), *Künstliche Intelligenz. Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?* (S. 269-286). Mohr Siebeck.

Singelnstein, T. (2018). Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention. *Neue Zeitschrift für Strafrecht, 38*(1), 1-9.

Singelnstein, T. (2020). Preventive Turn. Wie Gefahr und Risiko zum zentralen Gegenstand von Strafrecht und sozialer Kontrolle werden. In T. Fischer & E. Hilgendorf (Hrsg.), *Gefahr* (S. 95-112). Nomos.

Singelnstein, T., & Kunz, K.-L. (2021). *Kriminologie. Eine Grundlegung, 8. Aufl.* utb.

Sommerer, L. (2020). *Personenbezogenes Predictive Policing*. Nomos.

Sonka, C., Meier, H., Rosseger, A., Endrass, J., Profes, V., Witt, R., & Sadowski, F. (2020). RADAR-iTE 2.0: Ein Instrument des polizeilichen Staatsschutzes. Aufbau, Entwicklung und Stand der Evaluation. *Kriminalistik, 74*(6), 386-392.

Spranger, M., & Labudde, D. (2020). Vorhersage von Gruppendynamiken auf der Grundlage von Daten aus Sozialen Netzwerken. In T.-G. Rüdiger & P. Bayerl (Hrsg.), *Cyberkriminologie* (S. 653-683). Springer.

Sprenger, J. (2020). Verbrechensbekämpfung. In M. Ebers, C. Heinze, T. Krügel & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik. Rechtshandbuch* (S. 961-986). C.H.Beck.

Ulbricht, L., & Egbert, S. (2024). In Palantir we trust? Regulation of data analysis platforms in public security. *Big Data & Society*, *11*(3), 1-15.

Volkmann, U. (2021). Prävention durch Verwaltungsrecht: Sicherheit. *Neue Zeitschrift für Verwaltungsrecht, 40*(19), 1408-1415.

Wehrheim, J. (2014). Definitionsmacht und Selektivität in Zeiten neuer Kontrolltechnologien. In H. Schmidt-Semisch & H. Hess (Hrsg.), *Die Sinnprovinz der Kriminalität* (S. 137-153). Springer.

Zeit Online (2019, 08. Mai). *Yuval Noah Harari warnt vor möglicher Macht von Algorithmen.* **https://www.zeit.de/news/2019-05/08/yuval-noah-harari-warnt-vor-moeglicher-macht-der-algorithmen-**

190508-99-134593#:~:text=Hamburg%20(dpa)%20%2D%20Der%20israelische,könnten%2C%20als%20sie%20sich%20selbst. Zugegriffen: 08.08.2024.

Zwick, M. (2020). Risikoakzeptanz und Gefahrenverhalten. In T. Fischer & E. Hilgendorf (Hrsg.), *Gefahr* (S. 29-54). Nomos.