Lucia Sommerer: Personenbezogenes Predictive Policing. Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose

von Prof. Dr. Anja Schiemann

2020, Nomos, ISBN: 978-3-8487-6233-01, S. 400, Euro 104,00.

Prognosesoftware wird für die Polizeiarbeit auch in Deutschland schon seit einigen Jahren eingesetzt. Den Verheißungen auf Steigerung der Effizienz und Objektivität der Polizeiarbeit stehen auf der anderen Seite rechtliche Bedenken gegenüber, die eine solche Automatisierung der Kriminalitätskontrolle gerade auch durch den Einsatz personenbezogener Daten mit sich bringt. Insofern ist es verdienstvoll, dass sich *Sommerer* nicht nur den Grundlagen des personenbezogenen Predictiv Policing widmet, sondern auch dessen rechtlichen Grenzen. Zudem wird eine kriminologische, soziologische und rechtstheoretische Analyse vorgenommen und Empfehlungen für Mindestanforderungen an die algorithmengestützte Straftatprognose ausgesprochen.

Zunächst beleuchtet die Verfasserin die technischen Grundlagen, wobei eine Übersichtstabelle zum Vergleich traditionell statistischer und algorithmengestützter Kriminalprognosen die Divergenzen deutlich macht (S. 59). Durch die Ausführungen wird herausgestellt, dass bereits regelbasierte algorithmische Entscheidungssysteme zentrale Neuerungen besonders für das Anwendungsstadium eines Kriminalprognoseinstruments mit sich bringen. Fallbasierte algorithmische Entscheidungssysteme verändern dagegen den Prozess der Kriminalprognose von Grund auf. Dies bedinge Risiken und Herausforderungen für den Rechtsstaat (S. 73).

Es folgt eine Bestandsaufnahme des gegenwärtigen Einsatzes von Prognosesoftware, wobei zunächst die USA und Großbritannien in den Blick genommen werden. Sodann wird sich für den deutschsprachigen Raum mit vier Entwicklungen näher befasst. Dabei handele es sich bei RADAR-iTE und hessenDATA um Vorstufen des Predictive-Policing, bei DyRiAS und dem Fluggastmusterabgleich könne hingegen bereits von personenbezogenem Predictive-Policing gesprochen werden (S. 83). Auch hier wird anhand einer Tabelle deutlich gemacht, wie der Daten-Input, die Verarbeitung und der Daten-Output bei diesen 4 Prognoseprogrammen aussieht (S. 84), bevor sich den Programmen im Einzelnen gewidmet wird.

Die Verfasserin stellt fest, dass der Fluggastdatenabgleich die größte Streubreite und somit die größte Nähe zu den flächendeckenden Predictive-Policing-Ansätzen der USA aufweist. Aber auch hessenDATA wohne das Potenzial einer großen Streubreite inne. Während diese beiden Ansätze in die Kategorie Big Data und Machine Learning einzuordnen seien, stellten DyRiAS ein regelbasiertes Predictive-Policing-System und RADAR-iTE eine noch schlichter umgesetzte Vorstufe des Pedictive-Policing dar.

Letztlich seien aber alle vier Instrumente entwickelt worden, um durch Laien ohne besondere psychologisch-kriminologische Ausbildung bedient zu werden. Schließlich käme auch die Anwendung polizeilicher Kriminalprognose auf psychisch Kranke in Betracht. Hierzu gebe es auch in Deutschland erste Bestrebungen (S. 99 f.).

Die Verfasserin hebt hervor, dass sich ein algorithmisches Modell nicht spontan aus einer Datengrundlage heraus ergebe, sondern es eines vielstufigen, von Menschen gesteuerten Prozesses bedarf, an dessen Ende das Modell stehe. Insoweit seien im Rahmen dieses Prozesses zahlreiche Wert- und Ermessensentscheidungen zu treffen, die rechtlich zu untersuchen seien.

Die rechtlichen Grenzen zeigt *Sommerer* dann in einem ersten Hauptteil in Kapitel 2 auf rund 150 Seiten auf und steckt zunächst den polizeirechtlichen Rahmen ab. Als erstes Zwischenergebnis hält sie fest, dass ein algorithmischer Risikoscore ein tatsächlicher Anhaltspunkt für das Vorliegen einer Gefahr sei, auf den aufbauend ein Mensch eine eigene Prognose zu treffen habe. Gelangt dieser zur Bejahung eines Gefahrenverdachts, so könnten Folgemaßnahmen zur Gefahrerforschung vorgenommen werden. Insofern seien Predictive-Policing-Programme nach derzeitiger Gesetzeslage nur als algorithmische Entscheidungsunterstützungssysteme für Menschen zu betrachten, nicht aber als den Menschen ersetzende eigenständig handelnde Entscheidungssysteme. Daher ersetzten solche Straftatenvorhersagen den Menschen nicht, sondern veränderten die Arbeit, die er zu leisten habe. Fehler im personenbezogenen Predictive-Policing führten demnach stets zur Rechtswidrigkeit einer darauf basierenden Maßnahme (S. 136).

Insofern wird eine Ermächtigungsgrundlage für den Einsatz solcher Systeme für erforderlich erachtet und im nächsten Untersuchungsschritt in den Polizeigesetzen gesucht. Die Verfasserin arbeitet knapp heraus, dass weder spezialgesetzliche Normen noch die allgemeine polizeirechtliche Generalklausel hierfür in Betracht kommen. Auch das Datenschutzrecht halte keine Ermächtigungsgrundlage bereit, allerdings erlaube der auf EU-RL 2016/681 basierende § 4 Abs. 1, 2 FlugDaG einen automatisierten Musterabgleich, jedoch nur für den Spezialfall der Fluggastdaten. Daher müsse das Fazit gezogen werden, dass weder für das Gefahrverdacht erzeugende noch für das Gefahrverdacht bestätigende personenbezogene Predictive-Policing, abgesehen vom Sonderfall des Flug-

DaG, eine Ermächtigungsgrundlage existiere (S. 153). Insofern müssten beim Einsatz entsprechender Systeme neue Rechtsgrundlagen geschaffen werden (S. 154), so dass *Sommerer* in einem nächsten Schritt den verfassungsrechtlichen Rahmen absteckt.

Hierzu untersucht sie die verfassungsrechtlichen Dimensionen des personenbezogenen Predictive-Policing mit Blick auf informationelle Selbstbestimmung, Diskriminierungsverbot, Transparenzgebot und Unschuldsvermutung. Nach ausführlicher Wertung kommt die Verfasserin zu dem Ergebnis, dass dieses System nur dann eingesetzt werden könne, wenn sich eine Sachlage bereits auf eine konkrete Gefahr hin zugespitzt hat, jedoch die vermutlichen Täter noch unbekannt seien. Zusätzlich könne das personenbezogene Predictive-Policing zur Ressourcenallokation angewandt werden, wenn aus Sicht der Polizei bei mehreren Personen eine konkrete Gefahr vorliegt, jedoch nur Ressourcen zum polizeilichen Eingriff bei einzelnen Personen vorhanden sei (S. 169).

Hinsichtlich des Diskriminierungsverbots wird kritisch gesehen, dass es im Rahmen von algorithmischen Prognosen zu einer faktischen Umkehr der Argumentations- und Beweislast kommen könne. Den Betroffenen würde hier eine doppelte Darlegungslast einmal im Hinblick auf das Vorliegen einer Ungleichbehandlung und einmal im Hinblick auf die Widerlegung der statistischen Rechtfertigungen auferlegt. Angesichts der Komplexität sei hier zu befürchten, dass die gerichtliche Überprüfung zu einer Willkürkontrolle verkümmere und dem Staat auch im grundrechtssensiblen Bereich ein weiter Entscheidungsspielraum bei Auswahl und Bewertung von Korrelationen zugestanden werde. Dem sei entgegenzutreten, zumal das *BVerfG* von den Gerichten fordert, einen besonders strengen Rechtfertigungsmaßstab anzulegen (S. 193). Es müsse also sichergestellt werden, dass dem Staat weiterhin eine gesteigerte Darlegungs- und Beweislast zukomme, was in zwei Schritten erfolgen könne: Erstens habe eine stärkere Sensibilisierung des Rechts für statistisches, computerwissenschaftliches Wissen zu erfolgen und zweitens dürfe die Diskriminierungskontrolle von Algorithmen nicht individuellen Gerichtsverfahren überlassen bleiben, sondern müsse von einer unabhängigen staatlichen Stelle systematisch und präventiv vorgenommen werden (S. 194).

Bei der Untersuchung des Transparenzgebots beschreibt *Sommerer* zunächst die drei Schichten algorithmischer Intransparenz: die Unzulänglichkeit qua Geheimhaltung, die Unzugänglichkeit qua fehlendem Fachwissen und die Unzugänglichkeit qua systemimmanenter Komplexität (s. auch die Abbildung auf S. 200). Wichtig sei, alle drei Schichten der Intransparenz stets klar voneinander zu trennen (S. 205). Transparenz sei zum einen ex ante durch öffentlich zugängliche Registrierungserfordernisse aller Entscheidungen der Designphase und der abstrakten Wirkungsprinzipien des Algorithmus sicherzustellen. Diese ex ante Erfordernisse seien idealer Weise von einer zentralen staatlichen Kontrollstelle sicherzustellen, die Einsicht in Quellcode und Trainingsdaten des Algorithmus nehmen und bei Mängeln den Einsatz untersagen könne. Zudem seien ex post von der Kontrollstelle regelmäßige Algorithmenaudits durchzuführen, so dass Risiken minimiert und in rechtsstaatlich akzeptable Bahnen gelenkt werden könnten (S. 220 f.). Die Verfasserin plädiert dafür, personenbezogene Predictive-Policing-Systeme erst einzusetzen, sobald eine Kontrollstelle geschaffen worden ist (S. 240). Ein effektives Transparenzregime habe drei Säulen zu umfassen, nämlich Registrierung, staatliche Kontrolle und die Wahrung subjektiver Rechte (S. 241).

Schließlich wird der Frage der Vereinbarkeit des personenbezogenen Predictive-Policing mit der Unschuldsvermutung nachgegangen, aber sehr knapp und zutreffend ausgeführt, dass eine Anwendung der Unschuldsvermutung auf die Gefahrenabwehr schlicht nicht möglich ist. Allerdings bedeute dies nicht, dass der Staat pauschal ohne jegliche Schwellen von der Gefährlichkeit seiner Bürger ausgehen dürfe. Die Grenzen staatlichen Handelns im Bereich der Gefahrenabwehr seien aber insbesondere im Recht auf informationelle Selbstbestimmung zu suchen (S. 244).

In einem strafprozessualen Annex stellt *Sommerer* fest, dass mangels Rechtsgrundlage präventiv erstellte Risikoscores nach geltendem Recht nicht ins Strafverfahren importiert werden dürfen (S. 258).

Trotz dieser rechtlichen Limitierungen sei der Gesetzgeber nicht generell daran gehindert, solche Systeme einzuführen und der „Vormarsch … in Deutschland (dürfte) realpolitisch kaum aufzuhalten sein“ (S. 258). Daher wird die „algorithmische Wende in der Kriminalitätskontrolle“ (S. 260) in Kapitel 3 einer kriminologischen, soziologischen und rechtstheoretischen Analyse unterzogen. Hierzu wird zunächst ein Blick auf Vorfeldverlagerungen generell im Strafrecht geworfen und Normen wie § 89a und § 129a StGB unter dem Aspekt der Strafbarkeit im Vorfeld eigentlicher Rechtsgutsverletzungen kurz angerissen. Auch die Vorverlagerungen im Bereich strafprozessualer Ermittlungsbefugnisse seien zu beobachten, wie bspw. bei § 100b Abs. 2 Nr. 1 lit. a, b StPO oder § 81b Alt. 2 StPO. Daneben sei auch dem Sanktionenrecht eine Risikoorientierung immanent. Diese Tendenz zeichne sich auch in den Polizeigesetzen ab, bei denen vermehrt vom Erfordernis einer konkreten Gefahr abgerückt werde. Insofern wird resümiert, dass die zunehmende Fokussierung auf Risiken im Vorfeld von Rechtsgutsverletzungen sich faktisch für alle Gebiete der Kriminalitätskontrolle konstatieren lasse (S. 283).

Als Fazit zum dritten Kapitel merkt die Verfasserin an, dass der Einsatz personenbezogenen Predictive-Policing zwar aus rechtlicher Sicht nicht grundsätzlich zu untersagen ist, jedoch gerade hinsichtlich der tatsächlichen Auswirkungen in der polizeilichen Arbeit auch bei Einhaltung rechtlicher Rahmenbedingungen deutlichen Bedenken ausgesetzt ist. Die Anwendung komplexer neuer Technologien in der Kriminalitätskontrolle sei daher genau zu hinterfragen und bei Intransparenz zu untersagen (S. 341 f.).

Dementsprechend formuliert *Sommerer* in Kapitel 4 Empfehlungen für Mindestanforderungen an algorithmusgestützte Straftatenprognose. Differenziert wird hinsichtlich dreier Gebiete, nämlich den Entwicklungsmodalitäten, den Einsatzmodalitäten und Kontrollmodalitäten. Es sei entscheidend, dass die Mindestanforderungen nicht erst beim Einsatz von personenbezogenen Predictive-Policing-Systemen ansetzten, sondern bereits in der Entwicklungsphase, da hier die entscheidende Weichenstellung stattfände. So müsste sichergestellt werden, dass alle Entscheidungen des Entwicklungsprozesses eines solchen Systems in nachvollziehbarer Weise protokolliert werden. Diese Protokollierungspflicht umfasse die Auswahl der Trainingsdatenbasis, die Formulierung der Zielvariablen, d.h. welche Straftaten für welchen Zeitraum vorhergesagt werden sollen, die Auswahl der Inputvariablen und Entscheidungen in der Kalibrierungsphase des Lernprozesses. Insoweit müssten die Herkunft aller Datenquellen, die in die Trainingsdatenbasis einfließen, sowie die Auswahlerwägungen für die Inputvariablen festgehalten werden. Auch die Gewichtung der einzelnen Inputvariablen in einem Modell müsse protokolliert werden sowie der Cut-Off-Point, ab dem Personen als hochgefährlich eingestuft werden. Auch müsse ersichtlich sein, wie die Fehlerrate eines Systems kalibriert werde und wie in der Designphase auf das Verhältnis von falsch-positiven zu falsch-negativen Fehlern eingewirkt wird. Die Transparenz müsse dergestalt sein, dass es möglich ist, nachträglich die für einen erzielten Score entscheidenden Inputvariablen zu identifizieren und die Gewichtung zu bestimmten.

Darüber hinaus müsse die Unvoreingenommenheit des Algorithmus sichergestellt werden. Hierzu müsse bereits in der Entwicklungsphase im Trainingsdatensatz gezielt nach Diskriminierungen gesucht werden. Zudem seien die Gleichheit der Gesamtbetrachtung und Gleichheit der Fehlerhäufigkeit zu beachten und die Ergebnisse der Untersuchung zu protokollieren. Zur Beseitigung erkannter Diskriminierungen seien computerwissenschaftliche Methoden der „Ent-Diskriminierung“ anzuwenden.

Im Hinblick auf die Einsatzmodalitäten sei eine Rechtsgrundlage für das personenbezogene Predictive-Policing zu schaffen. Das System dürfe nur zur Entscheidungsunterstützung eingesetzt werden und nicht, um die eigene Gesamtbetrachtung und Entscheidung von Polizisten zu ersetzen. Zudem dürfe ein Riskoscore nicht flächendeckend und nur im Einzelfall und bei Vorliegen einer konkreten Gefahr für ein besonders bedeutendes Rechtsgut erfragt werden.

Auch bei der Kommunikation der Wahrscheinlichkeit einer Straftatbegehung seien verschiedene Aspekte zu beachten. So sei neben der Wahrscheinlichkeit einer Straftatbegehung auf die Fehlerraten des Systems hinzuweisen sowie die Basisrate der vorhergesagten Straftaten zu kommunizieren, also die Häufigkeit eines Delikts in der untersuchten Population und in der Gesamtbevölkerung. Darüber hinaus ist mitzuteilen, welche Inputvariablen das Ergebnis des Algorithmus im Einzelfall am stärksten beeinflusst haben.

Abschließend wird auf das Erfordernis der Etablierung von Kontrollmodalitäten für beide Stadien hingewiesen. Dabei habe sich die Kontrolle an der Transparenz bestehend aus öffentlicher Registrierungspflicht, subjektiven Betroffenenrechten und der Einrichtung einer staatlichen Kontrollstelle zu orientieren. Insofern seien die in der Entwicklungsphase des Algorithmus protokollierten Entscheidungen vor dem ersten Einsatz in öffentlich zugänglicher Weise bei einer Registrierungsstelle zu hinterlegen und Personen, zu denen ein Risikoscore erstellt wurde, die zentralen Inputvariablen für ihr individuelles Scoreergebnis mitzuteilen. Zudem muss ihnen die Möglichkeit gegeben werden, diesen Scorewert und eine darauf basierte polizeiliche Maßnahme gerichtlich anzugreifen.

Eine interdisziplinär ausgerichtete staatliche Stelle müsse schließlich eine Standardsetzung und systematische Kontrolle personenbezogener Predictive-Policing-Systeme vornehmen. Die Entwicklung und der Einsatz solcher Systeme sollte erst nach der Etablierung einheitlicher Standards vorgenommen werden. Die insoweit für die drei Komplexe ausformulierten Mindestanforderungen an algorithmengestützte Straftatenprognosen werden im Anschluss in einem guten Überblick zusammengestellt (S. 350). Hilfreich ist zudem, dass die Kernthesen der Dissertation in einem Abschlusskapitel nochmals zusammengefasst werden (S. 353 ff.).

Im Eingangskapitel wurde herausgestellt, dass der Weg des personenbezogenen Predictive-Policing mit unterschiedlichen Ansätzen in Deutschland längst beschritten wurde und in das Spektrum zwischen Gefahrverdacht bestätigendem und Gefahrverdacht erzeugenden Predictive-Policing fällt. Insofern sei der nächste Schritt zum personenbezogenen Predictive-Policing kein rein hypothetisches Szenario mehr. Die Verfasserin macht durch eine umfassende Würdigung aber deutlich, dass nicht alles, was technisch umsetzbar ist und Erfolg im Bereich der Strafverfolgung verspricht, auch rechtlich legitimierbar ist. Insoweit schafft die Dissertation von *Sommerer* nicht nur ein technisches Grundverständnis des Phänomens, sondern steckt – unter Einbettung der verfassungsrechtlichen Limitierungen – den rechtlichen Rahmen ab. Dabei wird deutlich, dass der Gesetzgeber gefordert ist, hier neue Vorschriften zu etablieren, die den verfassungsrechtlichen Implikationen Rechnung tragen und doch einen Einsatz mit Augenmaß legitimieren. Überzeugend sind insoweit auch die Empfehlungen für Mindestanforderungen an die algorithmengestützte Straftatenprognose unter Differenzierung nach Entwicklungs-, Einsatz- und Kontrollmodalitäten. An diesen Mindestanforderungen kann man sich orientieren, um auf einem organisatorisch und rechtlich gesicherten Fundament personenbezogene Predictive-Policing-Systeme zu schaffen. Ob all das, was sich *Sommerer* diesbezüglich wünscht, auch praktikabel ist, muss sich zeigen. Ganz sicher aber legt sie eine wertvolle Monographie vor, die einen ausgewogenen, aber auch kritischen Blick auf die „algorithmische Wende“ wirft und zur weiteren Diskussion anregt.