2009/49 Lifestyle

https://jungle.world/artikel/2009/49/nie-wieder-tatort

Software zur Kriminalitätsprävention

Nie wieder Tatort

Von **matthias monroy**

Die Europäische Union will realisieren, was Steven Spielberg mit seinem Film »Minority Report« fiktionalisierte: vorausschauende Kriminalitätsprävention. Neue Software soll so gut wie alle Daten bündeln, auswerten und interpretieren, damit die Behörden schon morgen wissen, was Herr Müller übermorgen tut. Die Sicherheitsindustrie freut sich auf die Investitionen.

In Spielbergs Science-Fiction-Thriller »Minority Report« liegen die drei dauerträumenden »Precogs« Agatha, Arthur und Dashiell in einem Becken mit Nährlösung. Ihre Köpfe sind verkabelt, denn ihre Träume sind wertvoll: Die Precogs träumen die Verbrechen der Zukunft, die Polizei muss nur die Prozesse in ihren Gehirnen auswerten, um die Verbrecher einzuknasten – und zwar, bevor diese ihre Taten begehen.
Die Pläne der Sicherheitspolitiker der EU gehen in dieselbe Richtung, nur ihre Realisierung fällt weniger esoterisch aus: Die vorausschauende Kriminalistik der EU soll nicht von träumenden »Precogs«, sondern ganz banal von Computertechnologie erledigt werden. Wenn die EU-Innen- und Justizminister im Dezember mit dem »Stockholmer Programm« ihren neuen Mehrjahresplan zur Inneren Sicherheit beschließen, dann bedeutet dies zunächst einmal weitreichende Investitionen in Produkte der europäischen Sicherheitsindustrie: in Überwachungstechnik, Hardware, Speichersysteme, Netzwerktechnik und Serverbetriebssysteme. Überwacht werden sollen damit vor allem zahlreiche Datenbanken. Die in ihnen verborgenen Informationen wollen die Verfolgungsbehörden mittels neuer Technologien für ihre Zwecke nutzbar machen.
Der globale Markt für jene Produkte aus dem Sortiment der »Homeland Defense« wird sich nach Schätzungen des Hamburger Weltwirtschaftsinstituts (HWWI) von 2005 bis 2015 auf 178 Milliarden US-Dollar vervierfachen. Nach Angaben der Studie mit dem Titel »Strategie 2030« würden rund 20 Prozent dieser Summe vom Sektor »Geheimdienstliche Aufklärung« abgeschöpft. Hiermit dürfte nicht nur der Ausbau der Geheimdienste gemeint sein, sondern vielmehr die verstärkte Anwendung nachrichtendienstlicher Methoden in der Polizeiarbeit. Der Studie zufolge bedarf es »des Ausbaus einer bislang nur rudimentär bestehenden Koordination von Auslands- und Inlandsdiensten mit Polizei- und Regierungsstellen«.
Um die Wettbewerbsfähigkeit der europäischen Sicherheitsindustrie zu fördern, hat die Europäische Union 2007 ein »Europäisches Sicherheitsforschungsprogramm« (ESRP) aufgelegt. Ungeachtet oftmals fehlender rechtlicher Grundlagen und jenseits von Datenschutzregelungen forschen in dessen Rahmen die »Abnehmer- und Anbieterseite« gemeinsam an neuen

Technologien zur vorausschauenden Überwachung. Ein Schwerpunkt des Sicherheitsforschungsprogramms ist die »Intelligente Überwachung«, eine Aufgabe ist dabei die »Integration, Zusammenschaltung und Interoperabilität von Sicherheitssystemen«. Technische Verfahren zur Erschließung und Auswertung »unstrukturierter Informationen« sollen zukünftige Risiken und potentielles abweichendes Verhalten analysieren. Die Softwareindustrie entwickelt dafür Anwendungen für Polizei und Geheimdienste, mit denen sich statistische Informationen und andere Daten automatisiert auswerten lassen – Programme für so genanntes data mining, wie sie bereits in einer Vielzahl von Unternehmen zur Steuerung logistischer Prozesse eingesetzt werden. Solche Programme versuchen, das Problem unterschiedlicher Dateitypen in den Griff zu bekommen: Texte, Webseiten, Verhörprotokolle, Zeugenvernehmungen, Observationsberichte, Audio-Mitschnitte der Telefonüberwachung, Faxe, Videos, E-Mails, Bewegungsprofile, Handy-Ortungsdaten, automatisiert gescannte Fahrzeug-Kennzeichen, georeferenzierte Daten und andere digitale Informationen. Denn seit dem 11. September 2001 zeichnet sich die fortschreitende Verschiebung von Polizeiarbeit hin zu einem »vorausschauenden Ansatz« ab.

Die Studie »Strategie 2030« freut sich daher schon auf massive Investitionen in diesen Bereich der Informationstechnologie: »Aus alledem wird klar, dass sich angesichts des erwarteten Marktvolumens enorme Chancen für Unternehmen bieten, die sich mit der Aufbereitung (Data mining), Analyse und Interpretation riesiger Datenmengen, der Entschlüsselung, der Vernetzung, aber auch der IT-Implementation und -Integration sowie der Schulung befassen.« Die Softwareindustrie ist für diese künftige Herausforderung bestens gerüstet. »Schon heute wissen, was morgen sein wird«, wirbt etwa der US-Konzern SPSS, einer der Marktführer für »Predictive Analytics«. Mittels behaviouristischer Analysen sollen Ermittler unterschiedliche Datentypen miteinander abgleichen können und so etwa Täterprofile entwerfen oder die Wahrscheinlichkeit zukünftiger Gesetzesübertretungen bestimmen. Die Software ist konzipiert für »Geldwäsche, Identitätsfeststellung, Drogenhandel, Terrorismus, Voraussage von Sicherheitsbedrohung«. Zu den Kunden zählen angeblich auch das Bundeskriminalamt (BKA), die meisten Landeskriminalämter und andere Polizeistellen. SPSS preist die Software als »Evolution in der Verbrechensbekämpfung«.
Ein weiterer, deutscher Anbieter »organisationsübergreifender Ermittlungskooperation« ist das Unternehmen Rola Security Solutions aus Oberhausen, das ein Ermittlungs- und Auswertungssystem für Polizei, Staatsschutz, Nachrichtendienste, Steuerfahndung sowie Privatunternehmen vorrätig hält. »Pünktlich zur WM« hatte Rola 2006 für seine Software eine Schnittstelle zur deutschen Inpol-Datenbank entwickelt und die »Anti-Terror-Datei« eingebunden. Rola-Software wird angeblich auch von deutschen Landespolizeien, dem BKA, der Bundespolizei und Steuerbehörden verwendet. Fraglich ist, wofür die Software von Verfolgungsbehörden wie dem BKA genutzt wird. Denkbar wären die einfache Vorgangsverwaltung, Ermittlungen oder Fallanalysen, aber auch – begründet mit der Abwehr von Terrorgefahr – ein permanenter Abgleich der mehr als 300 Datenbanken, die in der »Anti-Terror-Datei« zusammengefasst sind. Jörg Ziercke, Präsident des BKA, fordert seit langem einen »vorausschauenden Ansatz« für seine Behörde und formulierte dies in besonders kreativem Deutsch: »Wir müssen vor die Lage kommen.«

Um diesen prophylaktischen Ansatz technisch zu realisieren, wird im Rahmen des ESRP-Forschungsprogramms an zahlreichen Anwendungen gearbeitet, die auf der biometrischen Auswertung von Videoüberwachung und Satellitenaufklärung wie auch anderer »Sensoren«

basieren. Unter den 46 Projekten dieses Programms findet sich auch die automatisierte Erkennung abweichenden Verhaltens an öffentlichen Orten oder die Herausfilterung zurückgelassener Gepäckstücke. Mittels Simulationen wird auch versucht, menschliches Verhalten in Gruppen vorherzusagen.
Zur Suche nach »Gewalt«, »Bedrohungen« und »abnormalem Verhalten« im Internet forscht das Projekt »Intelligent information system supporting observation, searching and detection for security of citizens in urban environment« – kurz Indect –, das auch Bewegungsanalysen von Menschen, Fahrzeugen oder Schiffen ermöglichen soll. Indect will Webseiten, Chats, und Social Networks automatisiert durchsuchen und »automatische Dossiers« über Personen, Organisationen und ihre Beziehungen erstellen. An Indect ist auch die Universität Wuppertal beteiligt. Als der Wuppertaler AStA zusammen mit der Radikaldemokratischen Liste auf einem Gespräch mit den Projektverantwortlichen der Universität bestand, an dem dann auch der polnische Projektleiter teilnahm, wurde deutlich, dass die in Wuppertal entwickelten Anwendungen dazu beitragen sollen, mittels Kameras »deviantes Verhalten« aufzuspüren, etwa das »Zücken eines Messers«. Im Bereich Internet wurde die Forschung wie üblich mit der Suche nach Kinderpornographie begründet.
Während Universitäten und Sicherheitsfirmen an Technologien zur »automatisieren Kriminalitätsprävention« forschen, wird in zahlreichen Dokumenten der Europäischen Union von der Entwicklung eines »Intelligence-Led Law Enforcement« gesprochen. In deutschen Texten wird dieser Begriff mit »erkenntnisgesteuerte Strafverfolgung« übersetzt. Dieser auch von der EU-Kommission geforderte Ansatz orientiert sich an der Risikoanalyse, wie sie vom US-Heimatschutzministerium nach dem 11. September 2001 vorangetrieben wurde. Innerhalb der EU kommt hierbei der Polizeibehörde Europol eine Schlüsselrolle zu. Europol unterhält zahlreiche Arbeitsgruppen zur Risikoanalyse und gibt jährlich »Trend-Reports« zu Terrorismus und organisierter Kriminalität heraus.

Es gehört wenig Phantasie dazu, sich vorzustellen, dass europäische Polizeibehörden und Geheimdienste im Namen eines »Kampfes gegen Terrorismus und organisierte Kriminalität« und der Behauptung einer »konkreten Gefahr« regelmäßig und selbstverständlich innerhalb polizeilicher Datenbanken nach »Risiken« suchen. Anders sind die Begehrlichkeiten, auf Daten aus der Privatwirtschaft, darunter etwa Finanztransaktionen oder Passagierdaten, zugreifen zu können sowie Social Networks und Chats im Internet auszuwerten, nicht zu erklären. Werden diese Daten mit weiteren Informationen kombiniert, auf die Verfolgungsbehörden im Rahmen von Ermittlungsverfahren Zugriff erhalten – Informationen aus der Vorratsdatenspeicherung, abgehörte Gespräche, GPS-Daten –, kann dank der Ermittlungssoftware eine komplexe, dreidimensionale Graphik der sozialen Beziehungen von Verdächtigen und ihren Kontaktpersonen erstellt werden.
Die Problematik einer automatisierten, computergestützten »Vorhersage von Verbrechen« ist offensichtlich: Sie besteht nicht nur darin, dass, wenn Maschinen Personendaten prozessieren, um ihre Risiken zu interpretieren, aus datenschutzrechtlicher Sicht zumindest ein Einblick in die Funktionsweise und die Kenntnis abgefragter Datenbestände möglich sein sollte – sondern auch darin, dass die prophylaktische Verbrechensbekämpfung über kurz oder lang dazu führen kann, dass ein Staat seine Bürger nicht nur vorausschauend überwacht, sondern darüberhinaus ihr Verhalten durch die umfassende technische Kontrolle zunehmend normiert.