Der folgende Text ist eine für die FIfF-Kommunikation überarbeitete Version des Artikels "Minority Report", der bereits im Freispruch erschienen war.

Über den Wunsch, Überwachung zu automatisieren

Wenn Informatiker versuchen, Systeme zu bauen, die Politiker in Science-Fiction-Filmen toll fanden, so schafft den Sprung von der Fiktion in die Realität meist nur die Technik-Idee – die Technik-Kritik bleibt in der Regel unberücksichtigt.

Von Hollywood inspiriert...

Hier und jetzt beobachten kann man das an Steven Spielbergs Science-Fiction-Thriller Minority Report. Der Film spielt in einer Welt, in der modernste lebenserleichternde Geräte aber auch Überwachungs-Infrastruktur allgegenwärtig sind. Die Polizeibehörde Precrime besitzt das Mittel zur ultimativen Sicherheit. Verbrechen werden vorhergesehen und zukünftige StraftäterInnen ohne weiteren Prozess aus dem Verkehr gezogen. Systematisch wird jedoch der Bevölkerung und sogar den Agenten verheimlicht, dass es zu Fehlern kommt, dass Unschuldige verhaftet werden und Schuldige davonkommen.
Im Film kommen die Vorhersagen von drei hellsehenden, unter Drogen stehenden Kindern, deren Visionen direkt aus den Gehirnen auf Bildschirme übertragen werden. Da diese Art der Lösung nicht in Frage kommt, wird in der echten Welt daran geforscht, wie in Zukunft Computer die Voraussagen generieren können. Dazu werden Daten benötigt – viele Daten.

...von der EU finanziert

Eines von vielen dieser IT-Projekte zur Sammlung und Auswertung von Überwachungsinformationen ist das Forschungsprojekt INDECT, das seit Projektbeginn im Jahr 2009 mit fast 11 Millionen Euro von der EU finanziert wurde. Erklärtes Ziel von INDECT ist es, ein System für Sicherheits- und Polizeibehörden zu schaffen, das Informationen aus verschiedensten Quellen zusammenführt. Diese sind neben Überwachungskameras z. B. auch Gesichtsdatenbanken und Kommunikationsdaten, wie sie bei der Vorratsdatenspeicherung erhoben werden. Außerdem sollen Informationen aus dem Internet ausgewertet werden. Dazu gehört das Interpretieren sozialer Beziehungen und Profile in Diensten wie Facebook und Twitter und auch die Suche nach verdächtigen Inhalten in Foren, Blogs, auf Dateiservern, im Usenet und auf persönlichen Computern [1]. Einerseits sollen diese Datensammlungen als Informationsquelle für Polizeibeamte dienen, andererseits sollen sie von Computern automatisiert und in Echtzeit nach möglichen Gefahren und Auffälligkeiten durchsucht werden und Warnungen generieren.
Man könnte erwarten, dass ein so heikles Forschungsprogramm, das von der EU finanziert wird, Ergebnisse produzieren sollte, die tatsächlich angewendet werden können – unter anderem also mit den Grundrechten vereinbar sind. Um solchen Fragen und der Kritik am Projekt zu begegnen, hat INDECT eine sogenannte Ethik-Kommission eingesetzt. Man muss jedoch feststellen, dass diese Kommission lediglich die Rechtmäßigkeit und Ethik der Forschungsarbeit im Blick hat. Verletzungen der Grundrechte und Auswirkungen auf die Gesellschaft, die beim Einsatz der Forschungsergebnisse zu erwarten sind, werden rhetorisch umschifft oder ignoriert. In einer

Stellungnahme der Europäischen Kommission heißt es kurz: "Für die genaue Ausgestaltung und den rechtmäßigen Einsatz sind die Benutzer verantwortlich" [2]. Der Berliner Datenschutzbeauftragte Alexander Dix meint, derartige Projekte „drohen im Grunde Geld zu verschwenden, wenn die Ergebnisse hinterher nicht rechtskonform angewendet werden können.“ Ob solche Überwachungsmaßnahmen zum Einsatz kommen dürfen, hängt unter anderem davon ab, ob sie verhältnismäßig sind: Wie gut sie funktionieren, muss abgewogen werden gegen die Nachteile für Betroffene.

vom Glauben an zwei vermeintliche Wundermittel

Die Effektivität von Videoüberwachung zur Verhinderung von Straftaten und Vandalismus konnte bisher nicht mit Studien nachgewiesen werden. Dass Tausende von Kameras, wie z. B. in London, nicht die erhoffte Sicherheit gebracht haben, liegt meist nicht an der Qualität der Bilder oder fehlenden Aufnahmeperspektiven, sondern am Umgang der Überwachten mit den Kameras: Kriminelle planen die Kameras ein, bei Gewalt im Affekt werden Kameras oft einfach ignoriert; daran kann kein hochauflösendes Objektiv und keine zusätzlich aufgehängte Kamera etwas ändern. Dass der Ausbau von Videoüberwachung trotzdem weltweit vorangetrieben wird, kann nur auf einen starken, kaum zu begründenden Glauben an das Konzept Videoüberwachung zurückgeführt werden. Mit Scheuklappen für die grundsätzlichen konzeptuellen Mankos verbleiben nur zwei Dinge im Problembewusstsein der Befürworter:

1. Die Bilderflut, die wegen Personalmangel nicht ausreichend ausgewertet werden kann und
2. die Unzulänglichkeiten menschlicher Operateure bei der Bildauswertung.

Noch stärker als der Glaube an das Konzept Videoüberwachung scheint der Glaube an Technik zu sein, denn als Lösung der beiden Probleme gilt das von Entscheidern oft unverstandene und überschätze Wundermittel: der Computer. Er soll in den Videobildern nicht nur unerwünschtes Verhalten von Personen erkennen, sondern es auch vorhersagen.
Die Informatik versucht diese Aufgabe so zu lösen: Aus einer Folge von Pixeln (den Videoaufnahmen) soll eine Interpretation und Bewertung der Geschehnisse und letztlich ein Alarm errechnet werden. Dazu werden die bewegten Pixel zu Objekten zusammengefasst und durch Vergleich mit Modellen in Gegenstände und Personen eingeteilt. Bewegungen einzelner Körperteilen werden verfolgt, zusammengesetzt und typisiert: Rennen, Werfen, Lächeln. Für komplexere Bewegungen und Interaktionen mit anderen Personen und Gegenständen müssen komplexere Modelle gefunden werden.
Um Vorhersagen zu treffen, kann entweder die Abweichung von vorher definierter „Normalität“, oder die Übereinstimmung mit Modellen unerwünschter oder verdächtiger Geschehnisse gemessen werden. Ein paar Beispiele: Person A hat eine zu 78% aggressive Körperhaltung, Person B weicht beständig dem Sicherheitspersonal aus, Person D weicht vom üblichen Weg vom Check-In zum Gate 24 ab, Person E entfernt sich mehr als 3 Meter von Kinderwagen X, Person F verweilt auf dem Bahnsteig, obwohl bereits alle Linien ein Mal eingefahren sind, Transporter F, der sonst nie in der Gegen gesichtet wird sondern nur in fragwürdigen Randbezirken, hält direkt vor der Botschaft. Solche Modelle manuell zu erstellen, ist zeitaufwendig und teuer, daher wird auch die Automatisierung automatisiert. Computern wird beigebracht, selbstständig Modelle zu erstellen. In der Praxis geschieht das so: ein Algorithmus wird mit Videodaten gefüttert und dieser macht sich

dann selbst einen Reim auf die Pixel. Präsentiert man ihm 40 Stunden Videomaterial von „normalem“ Parkplatz-Geschehnissen, so soll eine Person, die in Stunde 41 von Auto zu Auto schlendert, dem Algorithmus als abweichend auffallen, ohne dass ein Mensch je darüber nachdenken musste, was genau an den vorherigen 40 Stunden „normal“ war. Nach diesem Verfahren, so wünscht man sich, sollen für beliebig komplexe Zusammenhänge und Geschehnisse Muster und Modelle erstellt werden.

10 Minuten im automatisiert überwachten Berlin 2023

Schaut man nicht nur auf Bildverarbeitung und künstliche Intelligenz sondern auch auf wissenschaftliche Veröffentlichungen der Biometrie, Kamera-, Sensor- und Netzwerktechnik, Textanalyse, Flugdrohnen, Datamining und Mensch-Technik-Interaktion so zeichnet sich anhand der vielen einzelnen Forschungsergebnisse jedoch das Szenario eines Systems ab, das weit über eine bildauswertende Kamera, die einen Alarm auslöst, hinaus geht:
Rebecca Schneider, 187 cm groß, rennt aus nur ihr bekannten Gründen im S-Bahnhof Ostkreuz den Bahnsteig entlang. Eine von tausenden über die ganze Stadt verteilten mit Rechenkapazität und Software ausgestatteten Kamera erfasst Rebeccas Bewegung. Anhand von Rebeccas Proportionen, dem Laufstil und Merkmalen ihrer Kleidung bekommt sie von der Kamera eine Identifikationsnummer zugeordnet und kann so über mehrere Kameras hinweg wiedererkannt werden. Im Vergleich mit zuvor automatisiert gelernten Modellen „normaler“ Bewegungen wird ihre Bewegung als auffällig der Stufe #5 klassifiziert und in Kombination mit der ID an einen zentralen Analyseserver übertragen. Stufe #5 führt noch nicht zu einem Alarm, ist aber schon hoch genug, so dass Rebecca genauer vom System beobachtet wird. Die Kameras in ihrer Umgebung beginnen höher aufgelöste Aufnahmen und ein genaues 3D-Modell ihres Körpers und ihres Ganges anzufertigen, für den Fall dass später etwas passiert und Beweise benötigt werden. Gleichzeitig wird an ihrem Laufstil und Rebeccas Gesicht ihre Identität über den Abgleich mit einer Biometriedatenbank festgestellt. In einem zweiten Schritt werden weitere Informationen von externen Informationsquellen abgefragt und analysiert. Rebecca kommt aus dem „Problembezirk Marzahn“, ihr Facebookprofil verrät, dass sie Mitglied der Facebookgruppe des als „gewaltbereit“ geltenden 1. FC Union Berlin ist. Außerdem hat sie in einem Internet-Forum Begriffe benutzt, die auch in Bekennerschreiben „militanter Gruppe“ verwendet wurden. All dies zusammen übersteigt einen internen Schwellwert des Überwachungssystems für Gefahrenpotential. Anhand des gespeicherten Videomaterials wird Rebeccas Laufweg, der letzten Stunden zurückverfolgt und festgestellt, dass sie in Charlottenburg (einem Bezirk in dem sich Marzahner statistisch gesehen mit geringer Wahrscheinlichkeit aufhalten) einen kleinen Gegenstand entgegen genommen hat von einer Person, deren Identifikation per Biometrie wegen Basecap und langem Mantel missglückt. Auch diese Tatsache lässt Rebecca in eine höhere Gefahrenkategorie aufsteigen.
In diesem Moment verlässt Rebecca den Bahnhof in Richtung eines leider noch nicht vollständig mit Kameras ausgestatteten Straßenzuges. Nur ein paar private Kameras von Imbissläden, die an das System angeschlossen sind, liefern hier Bilder. Einer Operateurin der auf einem riesigen Bildschirm wie in einem Computerspiel der ganze Bahnhof als Modell mit hineinprojizierten Videobildern angezeigt wird, wird vorgeschlagen, der für sie unkenntlich gemachten Person mit der Verdächtigkeitsstufe #7 und einem Gewaltpotential von 67%, die soeben den beobachtbaren Bereich verlässt, zu folgen. Die Operateurin gibt dem System wegen der zwei überdurchschnittlich hohen Zahlen und der Eiligkeit grünes Licht. Daraufhin wird eine autonome winzige Flugdrohne

gestartet, die Rebecca unbemerkt auf ihrem Weg begleitet um weitere Aufnahmen anzufertigen. Als sie in einen Hauseingang abbiegt und nicht weiter verfolgt werden kann, wird der Vorgang nach einer Weile des Wartens abgebrochen und, weil der Auffälligkeit nichts Ungesetzliches folgte, lediglich ein Vermerk zu Rebeccas ungewöhnlichem Verhalten in der Systemdatenbank abgelegt. Dieser wird bei der Einschätzung einer zukünftigen Situation, in der Rebecca involviert ist, berücksichtigt

So – oder so ähnlich gestaltet sich Überwachung in ein paar Jahren, wenn man die einzelnen Komponenten, an denen InformatikerInnen zurzeit forschen, zusammen nimmt. Schon jetzt ist in New York ein System vernetzter öffentlicher größtenteils aber privater Kameras mit Objekterkennung und Suchfunktion im Einsatz. Es können beispielsweise Anfragen gestellt werden, wie „zeige alle Menschen in der Nähe der Botschaft, die etwas Rotes tragen“.

Und das kostet's...

Da beobachtbares Verhalten nicht eindeutig interpretierbar ist, kriminelle Geschehnisse oder deren Anbahnung nicht unbedingt beobachtbar sind und obendrein Systeme niemals perfekt arbeiten können, kommt es zwangsläufig zu Fehlalarmen und nicht gegebenen Alarmen. Um die Genauigkeit der Alarme zu erhöhen, müssen eher mehr als weniger Daten erhoben und genutzt werden. Diese Notwendigkeit des Datensammelns und -auswertens ist mit den Datenschutzgrundsätzen wie z. B. Datensparsamkeit und Zweckbindung nicht vereinbar.

Doch wie das Beispiel Rebecca Schneider aus Marzahn zeigt, besteht nicht nur das Problem, dass das Recht auf informationelle Selbstbestimmung gefährdet ist. Es findet auch automatisierte Diskriminierung statt: Rebecca wird nicht nach ihrem tatsächlichen Verhalten beurteilt, sondern sieht sich auf Grund von automatisierter Kategorisierung, allein schon durch die intensivere Überwachung einer anderen Behandlung ausgesetzt als etwa Sophia Weidenfeld, 157 cm groß, aus Charlottenburg, die einen Blog übers Strohsternfalten schreibt; die jedoch ebenfalls über den Bahnhof rennt. Wissen Rebecca und Sophia über die Überwachung Bescheid, werden beide ihr Verhalten bewusst oder unbewusst an die vermeintlich hinter der Überwachung stehenden Norm anpassen. Sie können nicht prüfen, wie die öffentlich und privat erhobenen Daten verarbeitet werden, wie lange sie wo gespeichert werden und ob vielleicht auch an Orten überwacht wird, wo dies nicht ersichtlich ist. Durch die Möglichkeit der langfristigen Speicherung der erhobenen Daten, die auch Jahre später noch ausgewertet werden könnten, kann es sogar dazu kommen, dass sie an legitimen Geschehnissen wie Demonstrationen nicht teilnehmen, weil sie befürchten, dass die Teilnahme ihnen später oder von jemanden, der an die Daten gelangt, zum Nachteil ausgelegt wird. Vielleicht würde Sophia ohne solche Befürchtungen statt über Strohsterne über Asylpolitik schreiben.

Oft wird von Befürwortern solcher Systeme die Funktion der Operateure und OperateurInnen als Legitimation für eine umfangreiche Automatisierung dargestellt. Angeblich sorgen diese dafür, dass Betroffene keiner Beeinträchtigung durch automatisierte Entscheidungen unterworfen sind, wie es die europäische Datenschutzrichtlinie vorsieht. Tatsächlich jedoch sind die Entscheidungsprozesse in einem solchen System so komplex und verarbeiten so viele Informationen, dass die Entscheidungsfindung des Systems und mögliche alternative Interpretationen der Geschehnisse nicht für OperateurInnen nachvollziehbar dargestellt werden können. Hinzu kommt, dass bei Assistenz durch Computer aus psychologischen Gründen eine erhöhte Wahrscheinlichkeit besteht, dass der Empfehlung des Assistenzsystems ohne weitere Prüfung gefolgt wird, zumal wie in

Rebeccas Fall, die drohte außer Sichtweite zu geraten, oft Eile besteht, eine Entscheidung zu treffen.
Während wir also durch Automatisierung von Videoüberwachung eventuell ein nur geringes Maß an Sicherheit gewinnen, greifen wir stark in unsere Rechte ein und gefährden eine positive gesellschaftliche Entwicklung – Nutzen und Nachteil stehen nicht im Verhältnis.
Wenn derartige Techniken in Europa nicht zum Einsatz kommen dürften und die Investitionen in INDECT und anderen Forschungsbemühungen nicht umsonst gewesen sein sollen, dann müssten die Forschungsergebnisse entweder als Drehbuch-Idee für Minority Report 2 an Steven Spielberg verkauft werden oder aber exportiert werden in Länder, in denen innovationshemmende Bürgerrechte nicht ganz so genau genommen werden. Eines von beidem...

Quellen

[1] Dziech, Andrzej (2009): Präsentationsfolien zu INDECT, SRC'09 - Security R&D Innovations for the Citizens, Stockholm, 29.-30. September 2009. Abrufbar unter: http://www.src09.se/upload/Presentations/Day_1/Sessions-1100-1245/Session-1-Hall-B/Dziech.pdf.

[2] Europäisches Parlament (2010): Parlamentarische Anfrage E-3190/10 „Indect – Grundrechtecharta Art. 8" von Alexander Alvaro (ALDE), hier: Antwort von Herrn Tajani im Namen der Kommission. Abrufbar unter: http://tinyurl.com/euparlament-anfrage-indect.