Big Data Praxisbeispiel – Staatliche Überwachung

Auch der Staat verwendet Big Data in vielen Bereichen. Wenn es um die Sicherheit der Bürgerinnen und Bürger und die Abwehr von Gefahren geht, greifen Behörden, Polizei und Geheimdienste mitunter zu Überwachungs- und Auswertungsmethoden, die auf großen Datenmengen basieren. Woher die gesammelten Daten stammen, welche Schlussfolgerungen die Beteiligten aus ihnen ziehen und welche Kritik es gibt, erklärt der folgende Text.

Welche Beispiele gibt es?

Wenn Videokameras in Gebäuden, auf Plätzen oder in Verkehrsmitteln laufend bewegte Bilder aufzeichnen, erzeugen sie große Mengen an Film- und damit auch Datenmaterial. Gleiches gilt für die Überwachung der Internet-Kommunikation, also von E-Mails, Messengern und Social-Media-Kanälen. Mitunter greifen Ermittlerinnen und Ermittler auf die sogenannten Verkehrs- und Transaktionsdaten von Smartphone- sowie Computernutzerinnen und -nutzern zu. Sie beinhalten unter anderem Informationen zu Standorten, Bewegungen und genutzten Diensten.

Was hat das mit Big Data zu tun?

Die umfangreichen Daten werden durch Big-Data-Verfahren ausgewertet, um Zusammenhänge sichtbar zu machen, die für eine Person aus den Daten nicht ablesbar wären. Ausgangspunkt staatlicher Überwachungstechnologien ist meist der Wunsch, so früh wie möglich zu erkennen, ob und wo Gefahren für Menschen und Gebäude, das öffentliche Leben oder die Gesellschaft entstehen könnten. International sind verschiedene sogenannte „Pre-Crime"-Methoden bekannt, um Aufstände oder Verbrechen vorherzusagen. Dazu zählt auch, durch mehr oder weniger direktes Eingreifen rechtswidrige und kriminelle Handlungen zu verhindern, etwa durch Polizeieinsätze oder verdeckte Ermittlungen. Dabei werden Kriminalitätsstatistiken mit Wohngegenden, sozialen Milieus und weiteren Faktoren kombiniert, um hochzurechnen, mit welcher Wahrscheinlichkeit bestimmte Delikte vorkommen.

Welche Institutionen arbeiten in diesem Bereich mit Big-Data-Anwendungen?

Als Datensammler für den deutschen Staat sind Staatsanwaltschaften und Polizei zuständig, aber auch der Zoll und Institutionen des Grenzschutzes. Darüber hinaus sind Geheimdienste mit unterschiedlichen Kompetenzen und Verantwortungen, wie der Bundesnachrichtendienst (BND), der Militärische Abschirmdienst (MAD) und der Verfassungsschutz als Big-Data-Verwerter tätig. Auch die Steuerfahndung bedient sich bestimmter Datensammlungen und -auswertungsmethoden. Die jeweils anwendbaren Gesetze bestimmen dabei, welche Daten für wie lange und unter welchen Bedingungen gespeichert und ausgewertet werden dürfen. Gerade, wenn es um Strafverfolgung geht, ist es im Normalfall notwendig, dass eine Richterin oder ein Richter das Vorgehen geprüft und genehmigt hat. Um die Tätigkeit der Geheimdienste auf ihre Rechtmäßigkeit hin zu überprüfen, wurden im Bundestag und in den Landesparlamenten entsprechende Ausschüsse eingerichtet.

Kritik an der Überwachung

Zu Kritik kommt es immer wieder, wenn staatliche Einrichtungen massenhaft Daten von Bürgerinnen und Bürgern sammeln und speichern. Auf diese Weise entstehe, so das Argument, zu viel Daten-„Beifang", also Tausende und Abertausende personenbezogene Daten von unschuldigen Bürgerinnen und Bürgern, die in den Datenbanken der Behörden landen.

Je mehr Daten hier anfallen, desto höher wird das Risiko falscher Verdächtigungen und fehlerhafter Erkennungen. Das lässt sich allein schon statistisch erklären: Weil eine Gesichtserkennungssoftware zu einem gewissen Prozentsatz Gesichter falsch zuordnet, geraten zwangsläufig auch unschuldige Menschen ins Visier der Überwachung. Je mehr Daten durch solche Software zum Einsatz kommen, desto mehr Menschen stehen fälschlicherweise unter Verdacht. Die Fehlerquote der eingesetzten Software bleibt zwar gleich, jedoch steigt die absolute Zahl der Verdächtigten.