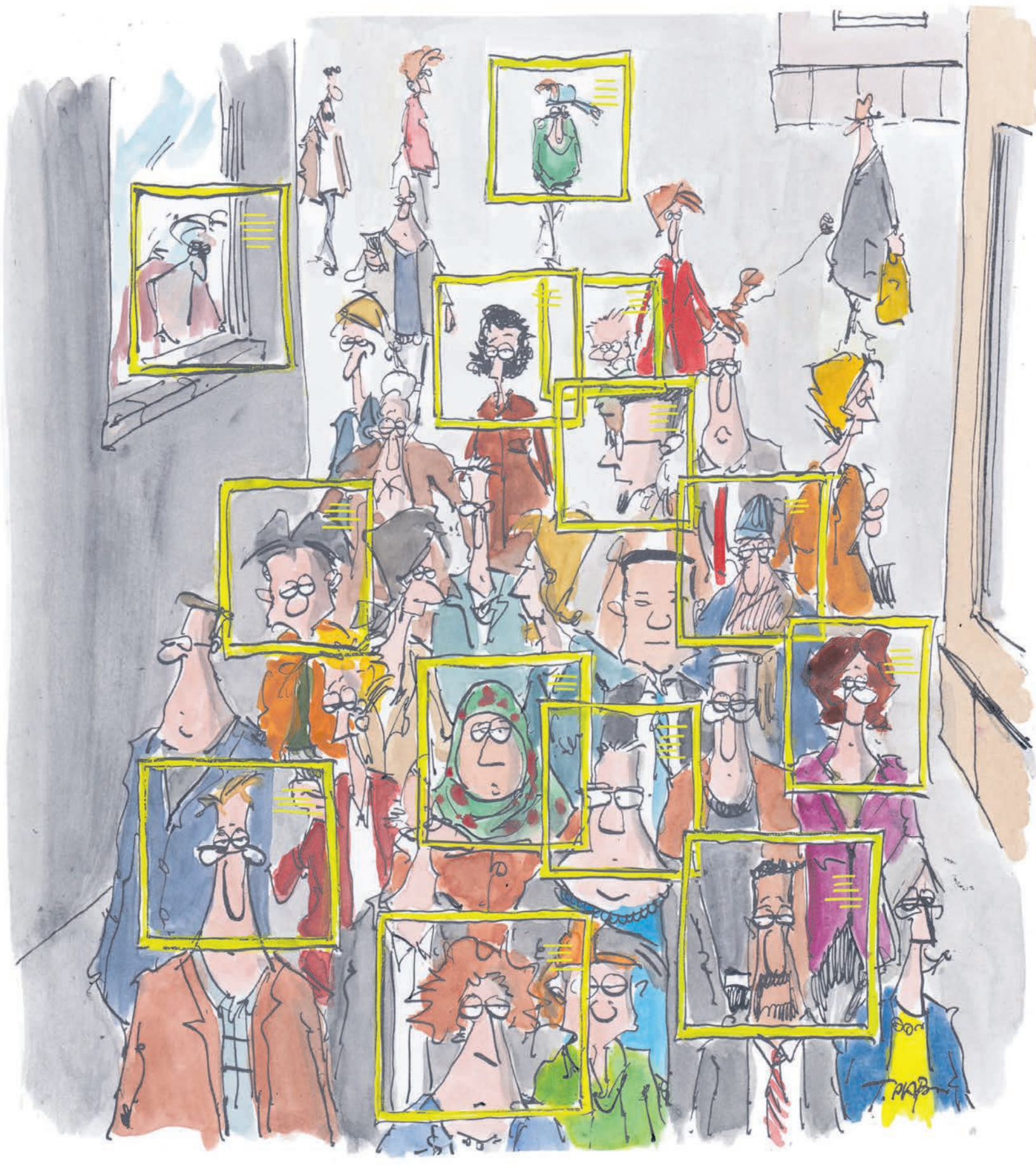
FrankfurterRundschau

UNABHÄNGIGE TAGESZEITUNG

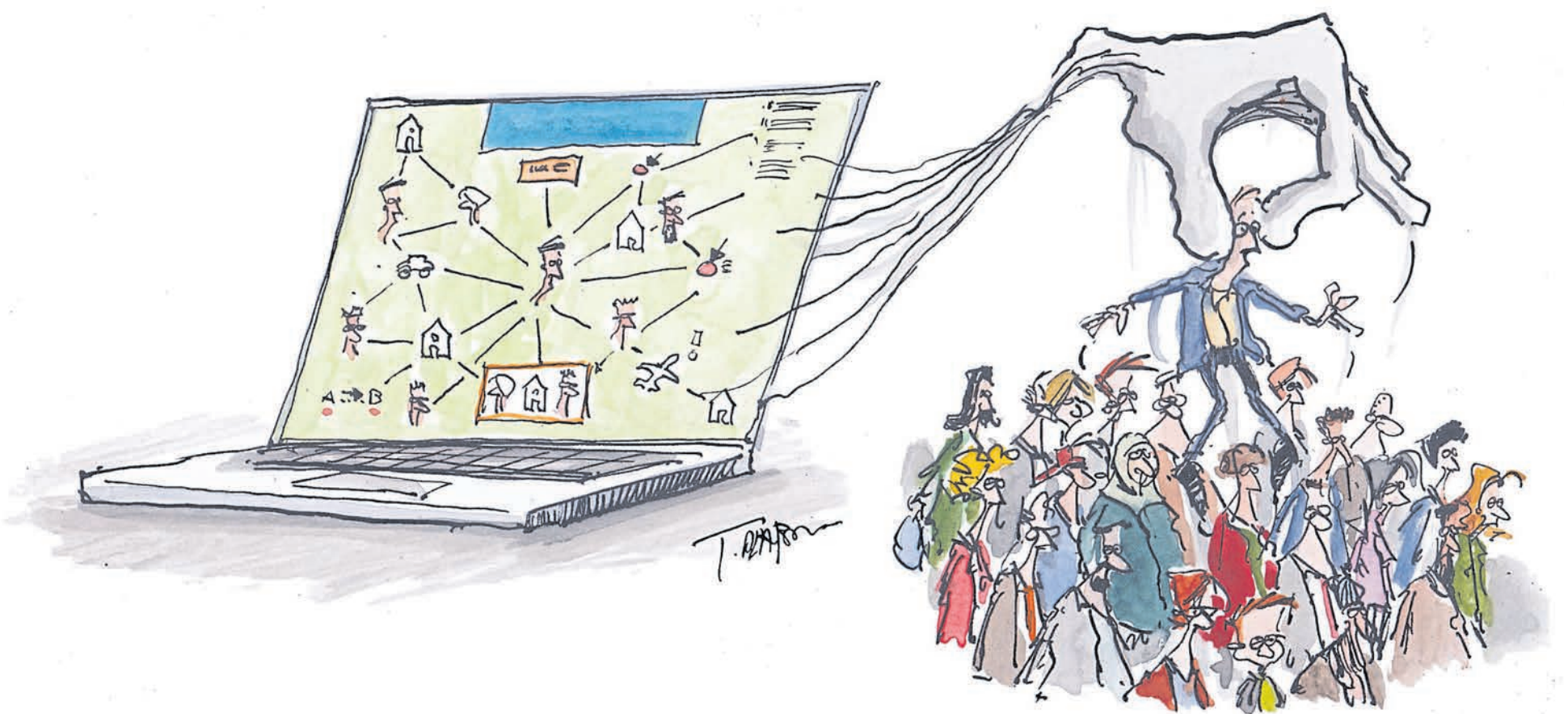


Automatisch verdächtig

Der Staat und die Daten: Ermittler setzen zunehmend auf Analysesoftware. Deren Einsatz verheißt Sicherheit – und birgt Risiken für uns alle.

Der Staat und die Daten

Teil I: Wie die Digitalisierung die Arbeit der Sicherheitsbehörden verändert



Polizei auf neuen Wegen

Die wachsende Menge an Informationen bereitet den Ermittlern Kopfzerbrechen. Um besser durchzublicken, setzen sie umstrittene Software ein. Die Folgen dieser Entwicklung sind nicht absehbar

Von Ruth Herberg und Alicia Lindhoff

Auch im Jahr 2020 arbeitet man im „Tatort“ noch weitgehend analog. Im öffentlich-rechtlichen Krimi pinnen Ermittler Bilder von Verdächtigen an die Wand und ziehen mit einem Edding Verbindungen zwischen ihnen. Wer zum Innendienst verdonnert wird, muss sich durch Unmengen an Ordnern wühlen, und Zusammenhänge zwischen relevanten Informationen suchen.

Bei der Polizei in Nordrhein-Westfalen übernimmt demnächst der Computer in Teilen diese Arbeit. Vor wenigen Tagen wurde bekannt, dass die Beamtinnen und Beamten bald mit einer Datenanalyse-Software des US-Unternehmens Palantir arbeiten werden. Geht es um schwere Straftaten, soll das Programm unterschiedliche Daten – nicht nur polizeiliche – und Informationen aus sozialen Medien zusammenführen und sie auswerten.

In Hessen ist Palantir bereits präsent. Das US-Unternehmen bekam am 31. Mai 2017 den Zuschlag für den Einsatz seiner Analyse-Software „Gotham“ bei der Polizei. Die nutzt die landeseigene Version „Hessendata“ seitdem nicht nur für Ermittlungen im Terrorismusbereich oder der organisierten Kriminalität, sondern auch bei Straftaten gegen ältere Menschen.

Palantir hat große Pläne. „Deutschland ist für uns ein Schlüsselmarkt“, betonte Laura Rudas im Gespräch mit dem „Handelsblatt“ schon vor knapp einem Jahr. Rudas ist bei Palantir unter anderem für die Geschäftsstrategie zuständig.

Ihre Worte wird manch ein Politiker und Polizist gerne hören. Laut einer Umfrage der FR halten die Innenministerien der Länder den Einsatz von Software zum Auswerten und Analysieren großer Datenmengen für nötig. Einige Länder setzen bereits auf entsprechende Verfahren und beobachten den Markt für solche Programme. Zwar gibt es auch deutsche Unternehmen, die sich darauf spezialisiert haben; allerdings gilt die Software von Palantir als die beste auf dem Markt. Und einige Bundesländer setzen bereits auf Palantir.

Das Unternehmen hat sich und seine Produkte im Landeskriminalamt Berlin und bei der Polizei Bremen vorgestellt. Und die Frankfurter Polizisten stellten gemeinsam mit Palantir-Vertretern im vergangenen November Mitarbeitern von Behörden aus Bayern, Hamburg und Thüringen das System „Hessendata“ vor.

Die Stärke von „Gotham“ liegt nach Angaben des Unternehmens in der Verknüpfung von strukturierten Daten wie Tabellen mit unstrukturierten wie Dokumenten oder Fotos. Die Software soll Zusammenhänge zwischen Objekten, Menschen und sogar Ermittlungen erkennen können, die der Polizist am Schreibtisch entweder gar nicht oder nur mit sehr viel mehr Aufwand finden kann. Sämtliche Daten verschiedener Quellen – auch sozialer Netzwerke – soll das Programm innerhalb kürzester Zeit automatisch analysieren und den Ermittlern so zum Beispiel detailliert alle Verbindungen einer Person liefern können.

» FR.DE

Der komplette dreiteilige Schwerpunkt als Download: www.fr.de/palantir

Über dieses Programm gibt es Streit. In Hessen versuchte ein eigens eingesetzter Untersuchungsausschuss zu klären, warum Innenminister Peter Beuth (CDU) ausgerechnet Palantir auswählte. Zudem ging es um die Frage, wie sicher die sensiblen Polizeidaten in der Software eines US-Unternehmens sind – eines Unternehmens, das zu Beginn auch mit Kapital einer Beteiligungsgesellschaft der CIA finanziert wurde. Fast alle Fragen blieben unbeantwortet. Doch die Regierungsparteien CDU und Grüne sehen trotzdem keine Unstimmigkeiten.

Michael Haug ist Bundesvorsitzender der Jungen Polizei in der Deutschen Polizeigewerkschaft. Seiner Einschätzung nach hat Datenanalyse-Software wie Palantirs „Gotham“ viel Potenzial. Gleichzeitig mahnt er, die digitale Souveränität Deutschlands nicht zu gefährden: Die Sicherheitsbehörden sollten eher mit öffentlichen Stellen wie Universitäten anstatt mit Unternehmen aus dem Ausland zusammenarbeiten, meint Haug. Nichtsdestotrotz werde es notwendig sein, auf Systeme zurückzugreifen, die die Polizei mit künstlicher Intelligenz unterstützen und ihr einen Teil der Arbeit abnehmen, denn: „Wir sind momentan fünf bis zehn Jahre hinterher.“

„Dem Produkt kann derzeit niemand das Wasser reichen“, sagt Bodo Koch bei einer Präsentation der Palantir-Software für die FR. Er leitet in Hessen den Einsatz der Software. Die hessische Polizei ist überzeugt, eine Art Pionier zu sein.

Ihr Projekt ist ein Beispiel für den Wandel der Polizeiarbeit. Die Aufgaben der Beamten verlagern sich zunehmend vor ein mögliches Verbrechen. „Vor die Lage kommen“ wird diese Verschiebung in Sicherheitskreisen genannt. Und hierbei spielen Datenanalyse-Programme eine wichtige Rolle, weil die Menge an Daten wächst, mit denen die Sicherheitsbehörden umgehen müssen.

Die noch jungen Änderungen der Polizeigesetze in mehreren Bundesländern stehen auch in diesem Zusammenhang. Dabei bekam die Polizei stets mehr Befugnisse, zum Beispiel bei der Überwachung digitaler Kommunikation oder im Umgang mit „Gefährdern“.

In Hessen wurde eigens ein Paragraf zur automatisierten Datenanalyse eingefügt. Die drastischste Veränderung: In vielen Bundesländern darf die Polizei künftig früher eingreifen. In Bayern beispielsweise muss für ein Einschreiten der Beamten in vielen Fällen keine konkrete Gefahr mehr vorliegen – es reicht eine „drohende Gefahr“.

Die Bürgerrechts-NGO Gesellschaft für Freiheitsrechte (GFF) hält diese Vorverlagerung der Zugriffsbefugnisse für verfassungswidrig – und klagt deswegen gegen mehrere der neuen Polizeigesetze, darunter auch das hessische. Auch die Änderungen zur automatisierten Datenanalyse sieht die NGO kritisch. In der Klagebegründung heißt es: „Wer in den Fokus einer Datenanalyse gerät, wird schnell zum gläsernen Menschen. Von der Analyse als Beifang mitbetroffen sind zudem zahlreiche weitere Personen: Die gleiche Adresse oder der gleiche Fußballverein können schon ausreichen, damit die Software Verbindungslinien zieht.“

Auch einzelne Straftaten wollen die Sicherheitsbehörden ganz gezielt vorhersehen – und dann verhindern. „Predictive Policing“, also vorhersagende Polizeiarbeit, heißt das. Doch in der Realität ist das nicht so einfach.

Dem sogenannten Profiling – also dem Erstellen von Profilen für bestimmte Personen – sind in Deutschland Grenzen gesetzt. Denn für die Verwendung von Daten gilt, dass der Staat persönliche Informationen von Bürgern

FR-SCHWERPUNKT – ALLE TEILE SCHON JETZT ZUM DOWNLOAD

Ab Oktober will die Polizei in Nordrhein-Westfalen die Software des US-Unternehmens Palantir testen und danach in ihren Alltagsbetrieb integrieren. Die hessische Polizei nutzt das umstrittene Programm zur Analyse von Massendaten bereits.

Ungeklärt ist: Was ist das für ein Programm? Wie funktioniert die Software, die in anderen Ländern schon viel Ärger provoziert hat? Und was bedeutet es, wenn die Sicherheitsbehörden auf automatisierte Analysen setzen? Diesen Fragen geht die FR in einer dreiteiligen Reihe nach.

Heute starten wir mit der Frage, warum der Einsatz solcher Software für die Polizei so attraktiv ist.

Im zweiten Teil (Donnerstag, 23.01.) stehen das Unternehmen Palantir und seine Software „Gotham" im Fokus: Der Firma eilt ein Ruf zwischen Dämonisierung und Glorifizierung voraus.

Im dritten Teil (Samstag, 25.01.) geht es um die Frage, welche Chancen und Risiken der Einsatz automatisierter Analysen bei Behörden birgt. Wohin diese Entwicklung im schlimmsten Fall führen kann, zeigt ein Blick nach China.

Alle Teile der Reihe stehen schon jetzt zum Download bereit. Unter fr.de/palantir können Sie den gesamten Schwerpunkt als PDF-Dokument herunterladen. thh

nur sparsam und möglichst zweckgebunden erheben und nutzen soll. Grundsätzlich darf die Polizei personenbezogene Daten nur so lange wie nötig speichern – also solange sie relevant sind. Ob das der Fall ist oder ob die Daten gelöscht werden müssen, soll regelmäßig überprüft werden: bei Erwachsenen alle zehn Jahre, bei Jugendlichen alle fünf und bei Kindern alle zwei Jahre. Zudem dürfen die Daten nur für den Zweck verwendet werden, für den sie erhoben wurden. Das ist ein Grund dafür, dass die Polizei die Informationen bislang in getrennten Datenbanken speichert.

Trotzdem kommt Programmen zur Auswertung von Falldaten wie dem von Palantir eine entscheidende Rolle zu. Auf Basis automatisierter Analysen sollen in den Datensätzen verdächtige Muster oder Verbindungen zwischen Personen, Orten, Gegenständen oder verschiedenen Ermittlungen erkannt werden; und zwar schneller und zuverlässiger, als der einzelne Beamte sie erkennen kann. Indem bestimmte Strukturen, Risikopersonen oder -orte früher identifiziert werden können, sollen die Sicherheitskräfte dadurch schon vor einer Straftat aktiv werden können.

Auch Airlines und Reisebüros übermitteln bereits umfangreiche Daten über Fluggäste an das Bundeskriminalamt (BKA). Das BKA darf die Daten fünf Jahre lang speichern und auf bestimmte Muster hin prüfen. So wollen die Beamten etwa herausfinden, wer einen Anschlag plant.

Mit Datenanalyse will die Polizei auch Einbrüche vorhersagen und verhindern, in einigen Bundesländern sind entsprechende Systeme im Einsatz. Sie errechnen auf Basis von Daten aus früheren Einbrüchen, mit welcher Wahrscheinlichkeit Diebe wann und in welcher Gegend zuschlagen könnten. Dort fährt die Polizei dann verstärkt Streife. „Solche Programme sind nicht der Weisheit letzter Schluss, aber es geht in die richtige Richtung", urteilt Polizeigewerkschafter Michael Haug.

Annette Brückner ist da skeptisch. Die ehemalige IT-Unternehmerin bloggt über die Informationstechnologie der Polizei und kritisiert die Entwicklungen in den Sicherheitsbehörden scharf. Sie glaubt, dass die „Vision von ‚Big Data' die Fantasien der Entscheider in den Führungsetagen von Polizeibehörden und ihren Innenministerien" verzerrt.

Die deutsche Polizei hinkt technisch hinterher

Gleichzeitig hinken die Informationssysteme der deutschen Polizeibehörden ihrer Meinung nach „krass dem Marktstand" hinterher. Dadurch, so Brückner, seien die Entscheider unter Druck – und entschieden sich im Zweifel für ungeeignete IT-Systeme.

Im Bundesinnenministerium arbeitet man derweil am großen Wurf: Die Informationsarchitektur der Polizei, die derzeit auf vielen verschiedenen Datentöpfen zu unterschiedlichen Deliktsbereichen basiert, soll vereinheitlicht werden. „Polizei 2020" heißt dieses Vorhaben, das – anders als der Name vermuten lässt – allerdings nicht in diesem Jahr umgesetzt wird. In dem Mammutprojekt sollen die zersplitterten Datensysteme der Polizeien von Bund und Ländern vereinheitlicht werden, aus vielen Töpfen soll einer werden. BKA-Präsident Holger Münch spricht gerne vom „Datenhaus der deutschen Polizei", das errichtet werde.

Um das Potenzial dieser neuen IT-Plattform auszuschöpfen, wollen Innenministerium und BKA Themenführerschaften vergeben: Einzelne Länder, Länderverbünde oder der Bund sollen für ein Thema verantwortlich sein, Entwicklungen vorantreiben und das Wissen mit den anderen teilen. Ob mit Themenführerschaft auch gemeint ist, verschiedene Softwareprogramme – wie etwa Palantirs „Gotham" – zu testen, ist bislang nicht bekannt. Eine „AG Analyse" gibt es aber.

Die hessische Polizei hofft, dass weitere Behörden die Software einsetzen werden. „Das BKA ist sehr interessiert an dem, was wir hier machen", betont Frankfurts Polizeipräsident Gerhard Bereswill. Man wolle ein Referenzmodell sein – er hoffe, dass irgendwann alle Bundesländer das Programm nutzen.

FANTASY UND REALITÄT

Palantir ist der Name eines US-Unternehmens, das sich auf die Analyse großer Datenmengen spezialisiert hat. Es bietet seine Dienstleistungen unter anderem Sicherheitsbehörden an. Der Name geht zurück auf die Fantasy-Saga „Herr der Ringe"; dort ist ein Palantir ein „sehender Stein", mit dessen Hilfe sich alles überwachen lässt.

In der Polizeiarbeit soll die Palantir-Software „Gotham" helfen, Verbindungen zwischen verschiedenen Personen, Vorfällen oder Daten zu erkennen. Die genaue Funktionsweise der Software bleibt aber intransparent. FR

KOMMENTAR

Ausgeblendete Risiken

Die Polizei will mit Hilfe von Software Verbrechen verhindern. Das ist ein Traum, der in einem Alptraum enden könnte.

Es gibt diese Formulierungen, bei denen man hellhörig werden sollte. „Ein neues Zeitalter" gehört dazu, klingt es doch nach einem wenig realistischen Versprechen – erst recht, wenn sich jemand in politischer Verantwortung so äußert. Zum Beispiel der hessische Innenminister Peter Beuth (CDU). Er behauptet, die Polizeiarbeit werde „in ein neues Zeitalter" gehoben – dank „Hessendata". Die Software kann riesige Mengen unterschiedlicher Daten strukturieren und analysieren, und mag tatsächlich eine Zeitenwende markieren. Allerdings eine riskante.

Politik und Sicherheitsbehörden in Hessen haben die Palantir-Software als für den Schutz der Bevölkerung nötige Investition verkauft, und als eine Art Wundermittel im Kampf gegen Terrorismus. Denn mit Hilfe von „Hessendata" wollen sie bis dato unentdeckte Zusammenhänge erkennen – und so potenzielle Täter identifizieren und Straftaten im Vorfeld verhindern. Die Hessen sind davon so begeistert, dass sie auch andere Länder und sogar das Bundeskriminalamt von der Software überzeugen wollen. Und tatsächlich hat man den Bedarf an Datenanalyse in den meisten Bundesländern längst erkannt. Erst vor wenigen Tagen ist bekannt geworden, dass auch die Polizei in Nordrhein-Westfalen bald mit der Palantir-Software arbeiten wird.

Von all dem bekommt die breite Öffentlichkeit nur wenig mit. Dabei ist der Einsatz des Programms unter den gegenwärtigen Bedingungen höchst problematisch. Beamtinnen und Beamte geben relevante Teile ihrer Tätigkeit – das Strukturieren von Informationen, das Suchen nach Verbindungen – an ein Computerprogramm ab, das eigenständig Datenbestände durchsucht und dann relevante Zusammenhänge präsentieren soll. Das Argument, dass die Polizeiarbeit damit wesentlich effizienter werde, mag stimmen. Die Frage ist allerdings, wie hoch der Preis dafür ist.

Nach wie vor ist zum Beispiel unklar, wie genau die Software arbeitet; welche Schlüsse die Beamtinnen und Beamten aus den Ergebnissen ziehen, die das Programm ausspuckt; ob und wie sichergestellt ist, dass bestimmte Gruppen nicht diskriminiert werden – denn Datensätze, in denen einzelne Gruppen von Menschen überrepräsentiert sind, sind verzerrt.

Wahrscheinlich wird Nordrhein-Westfalen nicht das einzige Bundesland bleiben, das dem hessischen Beispiel folgt. Spätestens dann muss in mehreren Punkten dringend nachgebessert werden. Zu viele Fragen sind noch offen.

Zum Beispiel, wer und wie den Einsatz der Analyseprogramme in den Sicherheitsbehörden kontrolliert. Geht es um Fragen der Nutzung und der Verwendung persönlicher Daten, werden gerne die Datenschutzbeauftragten als „Anwälte" der Bürgerinnen und Bürger ins Feld geführt. Sie kümmern sich darum, dass die Informationen, die genutzt werden, entsprechend der geltenden Datenschutzgesetze verarbeitet werden – dass die Behörden also etwa Löschfristen einhalten. Das ist richtig und wichtig. Was die Datenschutzbeauftragten allerdings nicht prüfen, ist zum Beispiel, in welcher Hinsicht diese Daten inhaltlich analysiert und welche Schlüsse daraus gezogen werden.

Es braucht daher eine zusätzliche, unabhängige Kontrollinstanz, die genau das überwacht. Das könnten die Parlamente auf Bundes- oder Landesebene übernehmen oder auch eine Art Ethikrat, in dem Juristinnen, Kriminologen, Soziologen, Psychologinnen, IT-Fachleute und zivilgesellschaftlichen Gruppen zusammenarbeiten.

Doch wer den Einsatz von Analyseprogrammen kontrollieren will, muss wissen, wie sie funktionieren. Es muss zum Beispiel klar sein, was die Beamtinnen und Beamten mit den Ergebnissen der Datenanalyse machen. Ob sie die Möglichkeit haben, sie zumindest stichprobenartig zu überprüfen oder ob sie dem Programm vertrauen müssen. Das kann auch transparent gemacht werden, ohne sensible Informationen herauszugeben. Das Gleiche gilt für die Frage nach der Datensicherheit – wie wird sichergestellt, dass keine polizeilichen Informationen abfließen? – oder die nach dem Schutz vor Diskriminierung.

Der Einsatz von Datenanalyse-Programmen wie Palantir muss deswegen auch transparenter werden. Nicht nur um der Kontrolle willen, sondern auch, damit die Bürgerinnen und Bürger für sich klären können, ob es für sie Sinn macht, viel Geld in solche Software zu investieren. Tatsächlich wäre dieses Geld – und hier geht es um Beträge in Millionenhöhe – woanders besser aufgehoben. Anstatt mit fragwürdigen Computerprogrammen die Straftaten Radikalisierter zu verhindern, sollte die Radikalisierung Einzelner verhindert werden.

Dem Extremismus kann (und muss) auf vielen Wegen entgegengetreten werden. Wäre es nicht mindestens genauso angemessen, in soziale Prävention zu investieren? Zum Beispiel in stärkere niedrigschwellige Angebote für Beratung und Gewaltprävention. In die Finanzierung von Projekten zur Demokratieförderung und Aussteigerorganisationen. In Programme zur Deradikalisierung, die es nicht nur offline, sondern insbesondere auch online geben muss. In Schulen als Ort für Debatten, an dem junge Menschen zum Diskutieren, zum selbstständigen Denken und zum Entwickeln von Haltungen angeregt werden. In soziale Sicherheiten wie eine abgesicherte Existenz und bezahlbaren Wohnraum. In Perspektiven für die Menschen.

Das alles klingt anstrengend und bei weitem nicht so aufregend wie eine hochmoderne Software, die Sicherheit auf Knopfdruck verspricht. In Wahrheit macht sie aber genau das Gegenteil: Anstatt Sicherheit zu schaffen, können auch unbescholtene Bürgerinnen und Bürger in den Fokus der Datenanalyse geraten und Menschen grundlos zu Verdächtigen werden.

Ist das die Zukunft, die wir wollen?

Ruth Herberg

Der Staat und die Daten

Teil II: Wie ein US-Unternehmen die Arbeit mit Big Data weltweit revolutionieren will

Vom Schlachtfeld in die Innenstädte

Die US-Firma Palantir entwickelt Software zur Analyse von Massendaten – und gibt so Sicherheitsbehörden ein mächtiges Werkzeug an die Hand

Von Alicia Lindhoff und Ruth Herberg

Wer „Herr der Ringe“ kennt, erinnert sich an den Zauberer Saruman. Hoch oben im Turm von Isengart plant er im Auftrag des dunklen Herrschers Sauron die Unterjochung von Menschen, Zwergen und Elben. Eine seiner mächtigsten Waffen im Kampf um Mittelerde: der Palantir. Wer einen solchen „sehenden Stein“ besitzt, kann damit die Welt bis in den hintersten Winkel überwachen und alles und alle im Blick behalten. Die ultimative Big Brother-Dystopie.

Kein Wunder, dass viele hellhörig geworden sind, als 2017 zuerst die hessische und Anfang dieses Jahres auch die nordrhein-westfälische Polizei verkündeten, eine Anti-Terror-Software der US-Firma Palantir zu kaufen. Eine Software, die noch dazu „Gotham“ heißt, wie die düstere Metropole aus den Batman-Comics.

Doch es sind nicht nur Namen, die das Misstrauen gegenüber den Datenanalysten aus dem Silicon Valley schüren. Vor allem in den USA macht Palantir immer wieder negative Schlagzeilen. Viele Mythen ranken sich um die Zusammenarbeit der Firma mit den US-Geheimdiensten CIA, FBI und NSA. Erst vor wenigen Monaten deckten Journalisten auf, dass die berüchtigte US-Immigrationsbehörde ICE 2017 in der Grenzregion zu Mexiko mithilfe von Palantir-Software Bewegungsprofile von minderjährigen Flüchtlingen und ihren Familienmitglieder erstellt hat, mit denen ihre Abschiebung erleichtert wurde. Die Firma hatte das zuvor bestritten und behauptet, der Behörde nur bei der Bekämpfung grenzüberschreitender Kriminalität zu helfen.

Und in Städten wie Los Angeles, wo die Polizei schon seit Jahren mit Palantir-Software arbeitet, beklagen Bürgerrechtler, das System verstärke diskriminierende Praktiken wie Racial Profiling oder führe dazu, ganze Stadtteile als Ghettos abzustempeln.

Was also hat die Verantwortlichen in Hessen und NRW dazu bewogen, Palantir den Vorzug vor weniger umstrittenen Software-Schmieden zu geben?

»FR.DE

Der komplette dreiteilige Schwerpunkt als Download: www.fr.de/palantir

Wie viele Sicherheitspolitiker vor ihnen dürfte sie vor allem die Aura von Genialität fasziniert haben, die die Entwickler aus dem Silicon Valley umgibt. Auch wenn Palantir nicht wenige Wettbewerber hat: Ihre Software gilt vielen in der Branche als das Beste, was der Markt derzeit zu bieten hat, wenn es darum geht, riesige Datenmengen aus den verschiedensten Quellen automatisiert zu analysieren. Die „Wirtschaftswoche“ nennt die Palantir-Software sogar „eins der mächtigsten Werkzeuge der Welt“. In Echtzeit erkennt die Software Muster in den Daten, die ein Mensch nur mit viel Glück und langer Recherche entdeckt hätte – wenn überhaupt. Von dieser Fähigkeit träumt in Zeiten, da das weltweit gespeicherte digitale Datenvolumen immer gigantischere Dimensionen annimmt, jede Behörde, jeder Geheimdienst, jedes Unternehmen.

Doch im Fall von Palantir liegen Glorifizierung und Dämonisierung dicht beieinander. „Palantir weiß alles über dich“, raunte der Mediendienst Bloomberg in einem Artikel über die Firma. Das US-Portal Slate.com hat das Unternehmen gerade erst auf Platz vier der gefährlichsten Tech-Firmen 2020 gewählt – nach Amazon, Facebook und Alphabet.

Die Anfänge der Firma, die auch gut 15 Jahre nach ihrer Gründung von vielen beharrlich als Start-up bezeichnet wird, sind eng verwoben sind mit George W. Bushs Krieg gegen den Terror nach dem 11. September 2001. Eine der frühesten Investitionen kam von In-Q-Tel, einer Tochterfirma der CIA, die Risikokapital für IT-Start-ups vergibt, um neue Technologien schnell für Militär und Geheimdienste nutzbar zu machen.

Palantir selbst lässt auf Anfrage wissen, das Ziel sei anfangs gewesen, den US-Behörden zu demonstrieren, „dass es im Kampf gegen Terrorismus weniger darum geht, immer neue Daten zu generieren, sondern die bereits rechtmäßig zugänglichen Daten besser zu nutzen“. Palantirs Datenanalyse-Werkzeuge wurden in Afghanistan und dem Irak eingesetzt und sollen angeblich geholfen haben, den Al-Kaida-Chef Osama Bin Laden ausfindig zu machen. Erst Anfang 2019 hat Palantir einen rund 800 Millionen Dollar schweren Vertrag mit dem US-Verteidigungsministerium unterzeichnet.

Palantir wirbt damit, dass ihre Software „Gotham“, die auch in Hessen und NRW zum Einsatz kommt, auf dem Know-How und der jahrelangen Erfahrung auf „Schlachtfeldern“ und in Einsatzzentren weltweit basiert. Doch wer steckt hinter dieser Firma, die Militärtechnologie in europäische Innenstädte bringt?

Peter Thiel, einer der bekanntesten Investoren der US-amerikanischen Techbranche, gilt als Genie und benennt seine Firmen gerne nach mächtigen Artefakten aus dem Tolkien-Universum. Der gebürtige Frankfurter war einer der ersten Kapitalgeber von Facebook und gründete zusammen mit Elon Musk den Bezahldienst Paypal.

Doch Thiel hat auch am meisten zum zwielichtigen Ruf der Firma beitragen. Der bekennende Libertäre hat an die ultrakonservative Tea Party und an Donald Trump gespendet. Er lehnt staatliche Regulierung ab und fordert, privatem Unternehmertum keine Grenzen zu setzen. In einem Essay schrieb er vor einigen Jahren, Freiheit und Demokratie seien unvereinbar. Thiel ist für europäische Staatsvertreter ein schwieriger Partner. Ganz anders sieht es bei dem anderen starken Mann hinter Palantir aus: Alex Karp.

Der 52-Jährige kombiniert seine Locken mit violetten Pullundern oder mit Sportkleidung, seine Mitarbeiter schult er im Tai Chi, und auf Podien wirkt er eher wie ein Intellektueller denn wie der Chef eines berüchtigten Tech-Unternehmens. Tatsächlich hat Karp in Frankfurt seinen Doktor in Philosophie gemacht. Theodor Adorno, Jürgen Habermas – es war die Anziehungskraft der Kritischen Theorie, die ihn an den Main lockte.

Ein Brachialkapitalist und ein eher linker Denker, der von sich selbst sagt, er habe einen „devianten“ Lebensstil und fürchte wenig mehr als das Ende der Privatsphäre: Was dieses wunderliche Paar verbindet, scheint neben einer staatskritischen Haltung vor allem die Lust am Dissens zu sein.

An ihr Kennenlernen im Studentenwohnheim der Eliteuniversität Stanford erinnerte sich Karp in einem Podcast, den er gemeinsam mit Springer-Chef Matthias Döpfner aufnahm: „Wir haben gerne diskutiert und gestritten.“

Dass der sonst sehr verschwiegene Karp ausgerechnet Döpfner Einblicke gewährte, ist kein Zufall. Seit Anfang 2018 sitzt er im Aufsichtsrat von Springer. Ende desselben Jahres berief ihn auch der Chemieriese BASF in seinen Beirat. Es folgte eine Charmeoffensive des Palantir-CEO in Deutschland. Innerhalb weniger Monate saß er bei der Münchener Sicherheitskonferenz auf einem Podium mit Ex-Verteidigungsministerin Ursula von der Leyen (CDU), plauderte bei einem Dinner zur Digitalökonomie mit Annegret Kramp-Karrenbauer (CDU) und sprach bei der „Digitising Europe“-Konferenz in Berlin. Karp nannte das deutsche Bedürfnis nach Datenschutz einen „Wettbewerbsvorteil“ und lobte, die hiesige „Talentbasis“ sei eine der besten der Welt.

Palantir braucht neue Absatzmärkte. Zwar gilt die Software-Schmiede als eine der höchstbewerteten Firmen des Silicon Valley. Doch auf der anderen Seite steht ein Geschäftsmodell, das

Peter Thiel. M. COHEN/GETTY IMAGES/AFP

Alex Karp. D. ANGERER/GETTY IMAGES/AFP

auch nach gut 15 Jahren des Bestehens keinen Gewinn abgeworfen hat. Der für 2019 heiß erwartete Mega-Börsengang ist auf unbestimmte Zeit verschoben. Und in den USA sind einige Kunden wieder abgesprungen, etwa Coca-Cola und American Express, aber auch die Polizeibehörden von New York und New Orleans.

Auch im asiatischen Raum fischt Palantir nach Kunden und Geldgebern. Europa bleibt aber ein besonders wichtiger Markt. Mittlerweile soll die Firma mehr Mitarbeiter in ihren Niederlassungen in London, Paris, München, Berlin und Amsterdam haben als am Stammsitz in Palo Alto. Laut Handelsregister ist der deutsche Hauptsitz ein Büro in Frankfurt, tatsächlich läuft in Deutschland wohl das meiste über die Niederlassung in München. Seit Monaten schreibt die Firma für das dortige Büro neue Stellen aus – von Softwareentwicklern über Personalverantwortliche bis hin zu Angebotsverfassern. Deren Aufgabe ist es, Palantir viele öffentliche Aufträge zu sichern.

Palantirs Stärke ist die Schwäche der anderen: Vielen Firmen und Behörden in Europa fehlt digitales Know-How – so dass die smarte Rhetorik der „Daten-Magier“ („Wirtschaftswoche“) oft verfängt. Palantir ist bekannt für seine subtilen Verkaufsstrategien. Während sie im Vergleich zu anderen Techfirmen selten auf großen Messen vertreten sind, gilt die Firma als besonders gut darin, in unverbindlichen Erstgesprächen einzelne Politiker, Behörden- oder Firmenvertreter von ihrer Technologie zu begeistern und zu Multiplikatoren zu machen.

Derlei Überzeugungsarbeit ist offenbar nötig. Grade in Deutschland, wo Datenschutz so groß geschrieben wird wie sonst kaum irgendwo auf der Welt, sind auch die Vorbehalte gegen den Einsatz einer Data-Mining-Firma, die mit US-Geheimdiensten zusammenarbeitet, immens. Dass Mitgründer Peter Thiel die Datenschutz-Grundverordnung als „dummes Eigentor“ der EU bezeichnet hatte, dürfte nicht geholfen haben, die Zweifel zu zerstreuen.

Hinzu kommt, dass Palantir sehr verschlossen ist. Interviews werden selten gewährt. Auf eine Anfrage der FR an Palantir Deutschland reagierte die Firma zwar schnell, schickte aber erst nach mehrtägiger Abstimmung mit dem Hauptquartier in Palo Alto ein PDF mit allgemeinen Informationen. Auch ein Telefonat lehnte die Presseabteilung ab. Stattdessen bot das Unternehmen ein Hintergrundgespräch an – vorausgesetzt, in der FR würde bis dahin nichts über das Unternehmen veröffentlicht. Das Gespräch fand nicht statt.

„Wir sind schlecht in der Werbung. Ich rede nicht gerne mit der Öffentlichkeit“, erzählte Karp im Podcast von Springer-Vorstandschef Matthias Döpfner. Wenn er oder andere Firmenvertreter es dann aber doch tun, dann sprechen sie davon, wie mithilfe ihrer Software Terroranschläge verhindert oder ein Kinderporno-Ring aufgedeckt wurden.

Mit autoritären Staaten will die Firma nicht kooperieren

Palantir präsentiert sich als idealer Partner für westliche Demokratien, die Sicherheit garantieren wollen, ohne auf Freiheit zu verzichten. Mit autoritären Staaten werde seine Firma niemals zusammenarbeiten, beteuerte Karp. Doch die Zweifel bleiben – auch innerhalb des Unternehmens. Einige Mitarbeiter in den USA fordert von Alex Karp, die Software nicht mehr in den Dienst der Einwanderungsbehörde zu stellen, solange dieser Bürgerrechtsverletzungen vorgeworfen werden.

Wieder kommt einem die Metapher in den Sinn, die die Firma mit ihrer Namensgebung selbst ins Spiel bringt. Der Zauberer Saruman kämpfte einst gegen den Tyrannen Sauron – zu diesem Zweck überließ ihm der Rat der Zauberer den Palantir. Erst als Saruman auf die Seite des Bösen wechselte, erkannten seine ehemaligen Verbündeten, welches Unheil der sehende Stein in den Händen der Falschen anrichten konnte.

WELTWEIT IM EINSATZ

Die Kunden von Palantir sind so unterschiedlich wie zahlreich. Neben der US-Immigrations- und Zollbehörde (ICE) gehören auch die US-Armee und die Polizeibehörden mehrerer Städte dazu – etwa das LAPD in Los Angeles.

In Europa nutzen Sicherheitsbehörden etwa in Deutschland, Frankreich, Dänemark, Großbritannien und den Niederlanden Software von Palantir.

Auch NGOs wie das Welternährungsprogramm der UN oder die Internationale Atomenergiebehörde (IAEA) setzen auf Analyse-Tools der US-Firma.

Viele privatwirtschaftliche Unternehmen nutzen ebenfalls die Dienste von Palantir. In Europa sind es etwa Airbus und Fiat Chrysler, aber auch der Konsumgüterkonzern Henkel, der Pharmariese Merck oder die Ölfirma BP. lic

FR-SCHWERPUNKT ZUM DOWNLOAD

Palantir gilt als eins der geheimnisvollsten Unternehmen der Welt. Die Software der Firma aus dem Silicon Valley ist für viele das Beste, was derzeit zu haben ist, wenn es um die Analyse von Massendaten geht. Gleichzeitig ist das Unternehmen umstritten, unter anderem wegen Verbindungen zu US-Geheimdiensten. In Deutschland nutz die hessische Polizei Palantirs Software „Gotham“, ab Oktober auch die Polizei von Nordrhein-Westfalen. Nach wie vor sind viele Fragen im Zusammenhang mit der Analyse polizeilicher Massendaten offen. Die FR greift diese Aspekte deswegen in einem Schwerpunkt auf.

Im heutigen zweiten Teil der FR-Reihe stehen das Unternehmen und seine Analyse-Software „Gotham“ im Fokus.

Im dritten und letzten Teil (Samstag, 25.01.) geht es um die Frage, welche Chancen und Risiken der Einsatz automatisierter Analysen bei Behörden birgt; wohin diese Entwicklung im äußersten Fall führen kann, zeigt ein Blick nach China.

Alle Teile der Reihe stehen schon jetzt zum Download bereit. Unter fr.de/palantir können Sie den gesamten Schwerpunkt als PDF-Dokument herunterladen. thh

„Massenüberwachung wird für die Polizei interessanter“

Aktivist Jesper Lund über den Einsatz der Palantir-Software bei der dänischen Polizei

Herr Lund, Dänemark ist das erste Land in der EU, das seine Polizei flächendeckend mit Palantir-Software ausgestattet hat. Die Firma wird oft mit „Predictive Policing“ – also „voraussagender Polizeiarbeit“ – in Verbindung gebracht. Ist das eine angemessene Beschreibung?

Die meisten Menschen denken, wenn sie „Predictive Policing“ hören, an den Film „Minority Report“ und den Versuch, Verbrechen vorherzusagen, bevor sie verübt werden. Meiner Einschätzung nach geht es darum bei Palantir nicht – zumindest nicht auf individueller Ebene. In den USA wird das zwar versucht, aber in Dänemark passt „Big Data Policing“ besser. Große Datenmengen werden automatisch analysiert, um Muster zu erkennen, die Ermittler möglicherweise nicht gefunden hätten. Diese Muster können auch darauf hinweisen, dass zum Zeitpunkt der Analyse Straftaten begangen werden. Insofern kann man doch von kurzfristigen Vorhersagemethoden sprechen. Es ist ein Paradigmenwechsel, der großen Einfluss auf die zukünftige Arbeit der Polizei haben wird.

Welchen denn?

Es bedeutet: weniger Polizisten auf der Straße, weniger Zeugenbefragungen, aber mehr Datenanalyse. Meiner Meinung nach wird außerdem die Massenüberwachung der Öffentlichkeit für die Polizei viel interessanter. Ohne solche Software hätten die Sicherheitsbehörden einen riesigen Bestand an unstrukturierten Daten, die Beamte selten für einen bestimmten Zweck verwenden können. Wenn sie jedoch zuvor unbekannte Muster automatisch aus der umfangreichen Datensammlung extrahieren können, dann wird das Programm für die Ermittler umso wertvoller, je mehr Daten sie sammeln.

Können Sie ein Beispiel nennen?

Eine Vorführung des Palantir-Programms bei der dänischen Polizei hat gezeigt, wie die Ermittler mit der Software ein Fahrzeug mithilfe von Live-Daten einer automatischen Kennzeichenerfassung überwachen können. Durch den Vergleich der Positionsdaten von Verdächtigen aus anderen Ermittlungen mit der Position der Kennzeichenscanner in Echtzeit erhält der Ermittler ein Bild davon, wer im Auto sitzt. Das hätte die Polizei ohne die Software nicht erkannt, wenn sie nur in ihrer Datenbank nach Nummernschildern gesucht hätte. Die massenhafte Installation von Kennzeichenscannern wird für die Polizei viel attraktiver.

Hat die Polizei mehr rechtliche Befugnisse zur Massenüberwachung bekommen?

Das dänische Parlament hat klargemacht, dass Palantir keinen Zugang zu verbotenen Quellen haben sollte. Was jedoch geändert wurde, ist die Zweckbeschränkung. Daten können jetzt für andere Zwecke als nur für die verwendet werden, für die sie ursprünglich erhoben wurden. Das war bisher nicht erlaubt, ist aber notwendig, um Daten aus verschiedenen Datenbanken zu verknüpfen. Außerdem wurden die Speicherfristen erheblich verlängert. Für verarbeitete Daten im dänischen Big-Data-System POL-Intel gilt jetzt eine neue Speicherdauer von zehn Jahren, die im Einzelfall sogar auf 18 Jahre verlängert werden kann.

ZUR PERSON

Jesper Lund ist Vorsitzender der dänischen Datenschutz-NGO IT-Pol und Mitglied der Vereinigung European Digital Rights (EDRI). ANDREEA BELU

Wo ist das Problem?

Angenommen, die Polizei scannt im Rahmen einer Ermittlung mehrere Tage lang die Kennzeichen aller Autos, die im Kopenhagener Stadtgebiet unterwegs sind. Früher hätten die sogenannten „No-Hits“, die für die aktuelle Ermittlung irrelevant sind, nach 30 Tagen gelöscht werden müssen. Werden ihre Daten jedoch im Big-Data-System der Polizei analysiert, können sie jetzt zehn Jahre lang gespeichert werden. In dieser Zeit können die Daten aller dieser Fahrzeuge für jede Bestimmung verwendet werden. Sie könnten also in einer Untersuchung zu einer Verdächtigen werden, nur weil Sie sich zu einer bestimmten Zeit in einem bestimmten Gebiet befanden. Das war vorher auch möglich, aber mit einem systematischen Data-Mining-Tool ist es viel wahrscheinlicher.

Gibt es in Dänemark Widerstand?

Nicht wirklich. Mit Ausnahme einiger Bürgerrechtsorganisationen wie unserer wird kaum darüber diskutiert. Viele Dänen haben volles Vertrauen in die staatlichen Behörden und in die Polizei. Zumal es selbst für Politiker und Journalisten schwierig ist zu erkennen, was die Gesetzesänderungen bewirken. Darüber hinaus bleibt die Datenerhebung meist unbemerkt. Viele Menschen werden auf der Grundlage ihrer Daten analysiert, ohne jemals offiziell als Verdächtige zu gelten. Es wird eine zunehmende Tendenz geben, Daten von allen Bürgern zu erheben, immer länger zu speichern und ständig Kontrollen und Abgleiche im Hintergrund durchzuführen – ohne dass wir uns dessen bewusst sind.

INTERVIEW: ALICIA LINDHOFF

Der Staat und die Daten

Teil III: Wie Behörden auf der ganzen Welt zunehmend Entscheidungen an Algorithmen abtreten

Ende der Unschuldsvermutung

Chinas Sozialkreditsystem kann den Alltag der Menschen im Land radikal verändern. Für die Uiguren geht es sogar um Leib und Leben.

Von Finn Mayer-Kuckuk

In der chinesischen Provinz Xinjiang läuft derzeit der weltweit größte Feldversuch mit Überwachung mithilfe automatisierter Massendatenanalyse. Der Staat schöpft alles aus, was machbar ist und bringt die neueste Technik in großem Stil zum Einsatz.

Auch andere Staaten setzen darauf – allerdings nicht zur lückenlosen Überwachung ihrer Bürger, sondern um mit den immer größeren Datenmengen umgehen zu können. Die hessische und die dänische Polizei nutzen etwa die umstrittene Analysesoftware „Gotham“ des US-Unternehmens Palantir, mit deren Hilfe sie Terroranschläge verhindern wollen; die Polizei in Nordrhein-Westfalen will bald nachziehen.

Wohin die automatisierte Analyse von Massendaten verschiedener Quellen im äußersten Fall führen kann, zeigt der Blick nach China. Dort werden die aus den Analysen gewonnenen Ergebnisse zum Erstellen von Risikoprofilen aller Bürger genutzt – also zur lückenlosen Überwachung.

Das Ergebnis ist erschreckend. Die Massenüberwachung beseitigt jede Privatsphäre. Eine Unschuldsvermutung gibt es nicht, alle Bürger stehen unter Beobachtung. „Die Auswirkungen auf andere Rechte wie die Ausdrucks- und Religionsfreiheit sind erheblich“, warnt die Organisation Human Rights Watch (HRW). Die Methoden richten sich derzeit gegen die muslimische Minderheit der Uiguren. Doch wenn die Technik sich als tauglich erweist, könne das Regime sie auf das ganze Land ausweiten, so HRW.

» FR.DE

Der komplette dreiteilige Schwerpunkt als Download: www.fr.de/palantir

Wer durch die Stadt Kashgar ganz im Westen des Landes läuft, sieht den Polizeistaat überall. Die blauen Uniformen der Polizei und die Flecktarnanzüge der Armee sind jedoch nur die oberflächlichen Anzeichen für das, was hier geschieht. Etwas mehr verraten schon die Überwachungskameras, die an jeder Ecke, in jeder Gasse an Masten und Halterungen übereinandergestapelt sind. Sie sind die Augen, mit denen die Computer unsere Welt überwachen. Die eigentliche Kontrolle findet auf Servern, in den Handys und den Rechnern der Polizei statt. Hier entstehen lückenlose Bewegungs- und Verhaltensprofile, hier verwaltet der Staat die berüchtigten Sozialpunkte.

Mehrere chinesische Firmen sind jederzeit bereit, Besuchern zu demonstrieren, was heute schon alles möglich ist. Horizon Robotics, Megvii, Intellifusion oder Sensetime gehören zu den globalen Spitzenreitern bei Gesichtserkennung und Verarbeitung der gewonnenen Daten. „Notfalls reicht auch ein Handyfoto als Vorlage“, sagt eine Megvii-Mitarbeiterin in Peking bei einer Vorführung des Programms „Face++“. Die Software kann beliebigen Personen durch die Netzwerke von Kameras im Stadtbild folgen. Den Anfang der Erkennung macht das Gesicht, doch die Software merkt sich am Bewegtbild auch den Gang und die Proportionen des Körpers, so dass sie einen Menschen auch von hinten

GUTE BÜRGER, SCHLECHTE BÜRGER?

Mit Sozialpunkten will die chinesische Regierung ihre Bürgerinnen und Bürger bald bewerten, um ihre Vertrauenswürdigkeit auszuweisen. Momentan laufen in mehreren Regionen des Landes Pilotprojekte, in denen das System in Teilen getestet wird. Ende dieses Jahres will sich Peking auf Details festlegen, um das Programm dann im ganzen Land zu starten.

Für das Scoring (Bewertung) werten Algorithmen Informationen aus staatlichen und privaten Datenbanken sowie Kameraüberwachung aus. In der Testphase gibt es etwa Punktabzüge für Regelverstöße, Verkehrsvergehen oder Zahlungsverzug bei Rechnungen. Auch allzu kritische Äußerungen in sozialen Medien könnten eines Tages dazu führen, dass jemand im Punktesystem nach unten rutscht, warnen Kritiker. Positiv bewertet werden dagegen etwa besondere berufliche Leistungen oder soziales Engagement.

Das Profil, das sich aus der Datenfülle ergibt, soll dann ganz konkrete Auswirkungen auf das Leben der Menschen haben. Behörden und Unternehmen könnten es abfragen, um Entscheidungen zu treffen. Von dem Punktestand könnte auch abhängen, wie schnell die Person Flug- oder Zugtickets oder ein Visum bekommt. Negative Bewertungen könnten außerdem höhere Steuern nach sich ziehen – oder Schwierigkeiten bei der Wohnungssuche, weil Menschen mit einem höheren Score bevorzugt werden.

Auch mit Gedankenlesen wird derzeit experimentiert. Medienberichten zufolge setzten einige Unternehmen entsprechende Technologien bereits im Testbetrieb ein – um die Arbeitsabläufe zu verbessern und die Produktivität zu steigern. Die Angestellten tragen Helme oder Mützen mit Sensoren, die mit Hilfe von Algorithmen und künstlicher Intelligenz Emotionen wie Traurigkeit, Angst oder Wut frühzeitig erkennen und messen sollen. Das Pilotprojekt „Neuro Cap“ beispielsweise wird demnach von der Regierung finanziert. thh/fmk/dpa

im Gedränge weiterverfolgen kann.

Die Rechner können ein komplettes Bild aller Bewegungen und Gewohnheiten zeichnen. In Regionen wie Kashgar, denen besondere Aufmerksamkeit gilt, registrieren die Kameras die Handlungen von fast allen Personen in ihrem Blickfeld. In ganz China ist solche Technik bereits im Einsatz, um das Wohlverhalten der Bürger zu bewerten.

In der südchinesischen Stadt Shenzhen beobachten die Kameras schon eine Reihe von Verkehrskreuzungen: Wer als Fußgänger bei Rot drüberläuft, wird erfasst. In Millisekungen sucht der Rechner aus der Bürger-Datenbank die Personalausweisnummer heraus. Er schickt dann eine ermahnende SMS an die Sünderin oder den Sünder und bucht ein Bußgeld vom Konto ab, berichtet die Zeitung „South China Morning Post". Wenn jemand mehrfach eine Straße bei Rot überquert, könne das auch die Sozialpunkte eines Bürgers beeinflussen, zitiert die Zeitung „Wang Jun", den Marketingchef von Intellifusion. „Dann könnte es für ihn auch schwer werden, einen Kredit zu erhalten."

Es entstehen zahlreiche einzelne Punktesysteme

Anders als in westlichen Medien oft berichtet, handelt es sich bei den Sozialpunkten nicht um ein umfassendes Gesamtsystem, das jeder Bürgerin und jedem Bürger eine Bewertung zuordnet. Es entstehen zahlreiche einzelne, zielgerichtete Sozialpunktesysteme von Behörden und Provinzen. Ihre Werte können jedoch aufeinander abfärben, wie das Beispiel der Verkehrssünder zeigt. Eine Fülle von Datenquellen dient dazu, Werte zu berechnen, die am Ende verschiedene Folgen haben können.

Nichts bleibt heute mehr unbemerkt. Während sich Regimekritiker früher noch mit etwas Glück im Café zusammensetzen konnten, ohne dass der Staatsapparat etwas von ihrer Begegnung mitbekam, schließen Chinas Behörden nun die letzten Lücken. Wenn die Polizei eine Person auf die Überwachungsliste setzt, erhalten die Beamten sofort eine Benachrichtigung, wenn diese ein vorher definiertes Gebiet verlässt. Wenn die Kameras die Bewegung nicht entdecken, registriert die GPS-Funktion des Handys sie.

Doch während für die meisten Menschen im Rest des Landes vielleicht ein etwas höherer Kreditzins droht, geht es für die Uiguren um Leib und Leben. Wer hier ins Fadenkreuz der Behörden gerät, muss ins Umerziehungslager, sieht seine Kinder vielleicht für Monate und Jahre nicht wieder. Dafür reicht ein falscher Scherz im Handy-Chat. Der große Bruder sieht, alles, hört alles und weiß alles.

56

PROZENT

der Deutschen sagen, dass sie kaum etwas über Algorithmen wissen

FR-SCHWERPUNKT ZUM DOWNLOAD

In einer digitalisierten Welt werden Entscheidungen zunehmend an Softwares und Algorithmen abgetreten – an Systeme also, die automatisch und eigenständig Daten analysieren und Entscheidungen treffen können. Das ist in der Wirtschaft der Fall, aber auch in staatlichen Stellen, vor allem in Polizeibehörden. In Deutschland nutzt die Polizei in Hessen seit rund zweieinhalb Jahren die Analyse-Software „Gotham" von Palantir, ab Oktober soll sie auch in Nordrhein-Westfalen getestet werden.

Viele Fragen im Zusammenhang mit der Analyse von Massendaten in staatlichen Stellen sind noch unbeantwortet. Die FR thematisiert sie in einer dreiteiligen Reihe.

Im heutigen dritten und letzten Teil geht es um die Frage, welche Chancen und Risiken der Einsatz automatisierter Analysen bei Behörden birgt. Wohin diese Entwicklung im äußersten Fall führen kann, zeigt ein Blick nach China.

Alle Teile der Reihe stehen zum Download bereit. Unter fr.de/palantir können Sie den gesamten Schwerpunkt als PDF-Dokument herunterladen. thh

73

PROZENT

der Deutschen sprechen sich laut einer repräsentativen Umfrage der Bertelsmann-Stiftung für ein Verbot von Entscheidungen aus, die von Algorithmen allein getroffen werden

„Das ist nicht per se schlecht"

Bürgerrechts-Aktivist Spielkamp über Predictive Policing, Sozialkreditsysteme in Europa und Intransparenz bei Palantir

Herr Spielkamp, für chinesische Bürgerinnen und Bürger kann es gravierende Auswirkungen haben, wenn sie im Sozialkreditsystem schlecht bewertet werden. Bei der Republica-Konferenz 2019 haben Sie einen Vortrag gehalten mit dem Titel „Bürger-Scoring in der EU – es passiert auch hier, nicht nur in China". Was meinen Sie damit?

Gemeint ist, dass es auch in Europa längst Behörden und öffentliche Institutionen gibt, die Bürger mithilfe von automatisierten, algorithmenbasierten Systemen bewerten. Auf dieser Grundlage werden Entscheidungen getroffen, die für die gesellschaftliche Teilhabe dieser Menschen relevant sind.

Sie haben diese Fälle in einem Bericht zusammengetragen. Besonders häufig kommen die Algorithmen im Bereich der Sozialsysteme zum Einsatz. Können Sie Beispiele nennen?

In Dänemark sollte ein System eingeführt werden, das auf Grundlage von Daten etwa zu Arbeitslosigkeit oder der Anzahl von Arztbesuchen das Risiko für Kindesvernachlässigung berechnet. Weil es sehr große Proteste dagegen gab, ist das Projekt zwischenzeitlich aber auf Eis gelegt. Der Arbeitsmarktservice in Österreich dagegen setzt nach wie vor einen Algorithmus ein, um die Arbeitsmarktchancen von Jobsuchenden zu bewerten – auf dieser Grundlage wird dann etwa entschieden, ob der Staat ihnen Weiterbildungen finanziert. Auch das wird allerdings kritisiert.

Warum?

Weil der Algorithmus bestimmte Vorurteile, die schon in der Gesellschaft herrschen, einfach perpetuiert. Frauen, die ein Kind haben, wurden zum Beispiel automatisch Betreuungspflichten zugewiesen, Männern aber nicht. Offenbar ist man davon ausgegangen, dass die Frau das in jedem Fall übernimmt. Das wurde dann entsprechend in den Algorithmus kodiert und damit diese bestehende Ungleichheit fortgeführt.

ZU PERSON UND SACHE

Matthias Spielkamp ist Mitgründer und Geschäftsführer der NGO Algorithm Watch. Der Journalist war mehrfach Sachverständiger in Bundestagsanhörungen, etwa zu künstlicher Intelligenz.

Algorithm Watch analysiert die Auswirkungen algorithmischer Entscheidungsfindungsprozesse auf menschliches Verhalten, ordnet sie ein und zeigt ethische Konflikte auf. In den Studien „Automating Society" und „Atlas der Automatisierung" trägt die Organisation Beispiele für algorithmenbasierte Systeme in Europa und Deutschland zusammen. fr

JULIA BORNKESSEL

Haben Sie auch ein Beispiel aus Deutschland gefunden?

Das Problem ist: Es gibt keine Möglichkeit herauszubekommen, wo die Verwaltung und die Behörden in Deutschland solche Systeme einsetzen, denn es gibt kein Register dafür. Wir finden, dass es so etwas geben muss. Es einzurichten ist allerdings aus zwei Gründen schwierig. Zum einen muss man klar abgrenzen, was da rein kommt. Für manche Leute ist schon Microsoft Excel oder die automatische Rechtschreibprüfung eine künstliche Intelligenz. Das ist ein Definitionsproblem, aber das lässt sich lösen.

Was ist der andere Grund?

Die Frage, was überhaupt „die Verwaltung" ist, also welche Stellen in das Register aufgenommen werden. „Verwaltung", das ist vom Bund bis zur kommunalen Ebene alles. Und alle sind unabhängig voneinander. Das rauszubekommen, ist eine Sisyphusarbeit. Aber wir müssen das anpacken. Nur so wissen wir, wo Risiken drohen.

Immer häufiger setzen Polizeibehörden Software zur automatisierten Datenanalyse ein, etwa um verdächtige Personen frühzeitig zu identifizieren – in Hessen das Programm „Gotham" von Palantir. Wo liegt aus Ihrer Sicht hier das Risiko?

Das, was Palantir anbietet, zählt ja zum sogenannten „Predictive Policing", also der vorhersagenden Polizeiarbeit. Das ist nicht per se schlecht; es könnte sogar Vorteile bringen, nämlich dann, wenn zum Beispiel versucht wird, bestehende Vorurteile und Rassismus zu neutralisieren; einfach weil das System eine evidenzbasierte Entscheidung ermöglicht. Deswegen sind wir nicht prinzipiell dagegen. Es kann aber auch den gegenteiligen Effekt haben und Diskriminierung verstärken – nämlich dann, wenn Sie auf Grundlage voreingenommener Datensätze zu voreingenommenen Prognosen kommen, ähnlich wie beim Beispiel des Arbeitsmarktservices in Österreich. Das muss nicht so sein – es kommt eben darauf an, wie es gemacht wird und welche Kontrollmechanismen existieren.

Reichen die Kontrollmechanismen in Hessen aus?

Nein, da fehlt es aus meiner Sicht an Transparenz. Palantir gewährt uns keinen Einblick. Es wird alles geheim gehalten, und der Souverän kann sich kein gutes Bild machen. Dazu kommt: Die Aufsicht führt in Hessen der Datenschutzbeauftragte. Aber für viele Probleme, die bei diesen Programmen auftreten können, hat der gar keine Handhabe. Er kümmert sich zwar darum, dass die bestehenden Gesetze zum Datenschutz eingehalten werden – aber zum Beispiel nicht, ob der Datensatz inhaltlich voreingenommen oder verzerrt ist.

INTERVIEW: ALICIA LINDHOFF UND RUTH HERBERG

VORSCHRIFTEN FÜR ALGORITHMEN?

Wenn Entscheidungen in der Wirtschaft oder in der staatlichen Verwaltung zunehmend an Algorithmen abgetreten werden, kann das Konsequenzen für Kunden oder Bürger haben. Trotzdem fehlt es für den Einsatz algorithmenbasierter Entscheidungssysteme bislang an konkreten Regeln und Leitlinien. Die Bundesregierung hat deswegen 2018 eine Datenethikkommission eingesetzt, die mittlerweile Handlungsempfehlungen für die Politik vorgestellt hat.

Der Umgang mit solchen Systemen soll sich künftig vor allem daran orientieren, welche potenziellen Auswirkungen sie auf den einzelnen Menschen haben. Je größer das Schädigungspotenzial eines Algorithmus ist, desto mehr Anforderungen sollten an das System und seine Betreiber gestellt werden – bis hin zu Verboten für Algorithmen, die ein „unvertretbares" Schädigungspotenzial haben.

Für weniger gefährliche Anwendungen schlägt die Kommission etwa eine Kennzeichnungspflicht vor, nach der der Betreiber deutlich machen muss, wann und in welchem Umfang ein algorithmenbasiertes System zum Einsatz kommt. Außerdem empfiehlt sie umfangreiche Offenlegungs- und Transparenzpflichten und Auskunftsrechte für Betroffene. Es sei zudem „erwägenswert", so die Kommission, den Anwendungsbereich des Antidiskriminierungsrechts auf automatisierte Datenauswertungen und Entscheidungsverfahren auszuweiten.

Werden in staatlichen Stellen Algorithmen eingesetzt, erfordere das „mindestens eine umfassende Risikofolgenabschätzung", empfiehlt die Kommission. Staatliche Entscheidungen, die durch den Einsatz algorithmischer Systeme zustande kommen, müssten transparent und begründbar bleiben. Dafür sollten unter Umständen die geltenden Informationsfreiheits- und Transparenzgesetze erweitert werden. thh

Für alle Neukunden:

Das Kombi-Abo print + digital!

FR+ FR

Inkl. Nutzung der FR-Apps für mobile Endgeräte von Apple und Android

Montags bis samstags in Ihrem Briefkasten:

- 6 Tage umfassend informiert
- Im handlichen Tabloid-Format
- Portofrei nach Hause
- Jede Woche 36 Seiten mehr Regionales
- 7 12-seitige Sonderausgabe „FR7“ in jeder Samstagsausgabe

+

Als digitale Zeitung und per App:

- Lesezeichen-Funktion nutzen und spannende Artikel teilen
- Ausgewählte FR-Artikel mit exklusiven Multimedia-Inhalten
- Regionale Inhalte selbst bestimmen
- AA Schriftgröße skalierbar und Zoom-Funktion
- Inhalte auch archivierbar – für PC, Tablet und Smartphone

+

Ihr Willkommens-Extra

USB-Stick, 16 GB

- Drehbarer Metallbügel zum Öffnen, Schließen und Schutz des USB-Steckers
- Metallöse ermöglicht die Anbringung an Schlüsseln

Sichern Sie sich jetzt alle Vorteile der FR – immer und überall:

www.fr.de/kombi

6PR19004

Ein Angebot der Frankfurter Rundschau GmbH, Frankenallee 71–81, 60327 Frankfurt am Main (HRB 36224, Handelsregister Frankfurt am Main), Telefon-Nr. (069) 21 99 30 00 (zum regulären Festnetztarif). E-Mail: vertrieb@fr-online.de. Das Angebot gilt ausschließlich für Neukunden. Eine Kündigung ist jederzeit mit einer Frist von 20 Tagen zum Monatsende bzw. zum Ende des vorausberechneten Bezugszeitraums möglich. Alle Preise gelten inklusive MwSt. und Zustellkosten im Inland. Es gilt das gesetzliche Mängelgewährleistungsrecht.
Widerrufsbelehrung – Widerrufsrecht: Sie haben das Recht, diesen Vertrag binnen 14 Tagen ohne Angabe von Gründen zu widerrufen. Ausführliche Informationen zum Widerrufsrecht unter www.fr.de/widerruf.
Apple, the Apple Logo, MacBook and iPad are Trademarks of Apple Inc., registered in the U.S. and other countries. App Store and AppleCare are Service marks of Apple Inc.

Impressum

Die Frankfurter Rundschau erscheint im Verlag der Frankfurter Rundschau GmbH.

Chefredaktion: Bascha Mika, Thomas Kaspar, Michael Bayer (Ressortleitung Digital)

Ressortleiter:
Politik/Panorama: Karin Dalka
Meinung: Andreas Schwarzkopf
Wirtschaft: Daniel Baumann
Sport: Jörg Hanau
Feuilleton: Christian Thomas
Frankfurt, Freizeit & RheinMain:
Stefan Kuhn, Georg Leppert (Stellv.)

Chef vom Dienst: Claudia Nenninger, Stefan Affentranger

Leitende Redakteure: Lutz Fischer, Claus-Jürgen Göpfert, Peter Hanack, Pitt von Bebenburg, Jan-Christian Müller

Redaktion: Mainzer Landstraße 205, 60326 Frankfurt am Main, Telefon 069/2199-1
Verlag: Frankenallee 71-81, 60327 Frankfurt am Main, Tel. 069/2199-1 (zugleich auch ladungsfähige Anschrift für die im Impressum genannten Verantwortlichen und Vertretungsberechtigten)

Internet: www.fr.de

Geschäftsführer: Dr. Max Rempel

Verantwortlich für Anzeigen: Dr. Thomas Baumann, Achim Pflüger, RheinMainMedia GmbH, Frankenallee 71-81, 60327 Frankfurt am Main, Telefon (069) 7501 – 33 36, Telefax (069) 7501 – 4105. RMM-Anzeigenpreisliste Nr. 24, gültig vom 1. Januar 2019 an.

Erscheint täglich außer sonn- und feiertags.

Monatsbezugspreis Inland: Trägerzustellung und Postbezug im gesamten Bundesgebiet 51,95 Euro; ermäßigter Bezugspreis für Studierende und Auszubildende (gegen Vorlage einer Bescheinigung) 26,95 Euro; alle Preise inkl. 7% Umsatzsteuer. Digitalabonnement 33,45 Euro; ermäßigter Bezugspreis für Studierende und Auszubildende (gegen Vorlage einer Bescheinigung) 26,95 Euro; alle Preise inkl. 19% Umsatzsteuer.
Monatsbezugspreis Ausland: auf Anfrage.

Bei Nichtlieferung ohne Verschulden des Verlages oder infolge höherer Gewalt keine Entschädigung. Für unverlangte Einsendungen übernehmen wir keine Verantwortung. Eine Verwertung der urheberrechtlich geschützten Zeitung und aller in ihr enthaltenen Beiträge sowie Abbildungen, insbesondere durch Vervielfältigung und/oder Verbreitung, ohne vorherige schriftliche Zustimmung des Verlages ist unzulässig und strafbar. Insbesondere ist die Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Zeitung in Datenbanksystemen ohne Zustimmung des Verlages unzulässig. Alle Rechte vorbehalten.

Druck: Frankfurter Societäts-Druckerei GmbH, Kurhessenstraße 4-6, 64546 Mörfelden-Walldorf.

Gerichtsstand: Frankfurt am Main.

Verleger bis 1973: Karl Gerold.

Die Frankfurter Rundschau GmbH (FR), hat die Erhebung, Verarbeitung und Nutzung der Abonnentendaten und sonstiger personenbezogener Daten aus ihrem Geschäftsbetrieb zu den jeweiligen vertraglichen Zwecken an die Frankfurter Allgemeine Zeitung GmbH, Hellerhofstraße 2-4, 60327 Frankfurt am Main übertragen. Der Zustelldienst ist an die Medienservice GmbH & Co. KG, Hellerhofstraße 2-4, 60327 Frankfurt am Main und weitere Zustellpartner übertragen, die hierfür von der FR die personenbezogenen Daten der Abonnenten erhalten. Betroffenenrechte wie das Recht auf Auskunft oder Löschung können stets gegenüber der FR geltend gemacht werden.

Die Inhalte dieser Zeitschrift werden in gedruckter und digitaler Form vertrieben und sind aus Datenbanken abrufbar. Eine Verwertung der urheberrechtlich geschützten Inhalte ist ohne vorherige schriftliche Zustimmung des Verlages unzulässig und strafbar, sofern sich aus dem Urheberrechtsgesetz nichts anderes ergibt.

© Alle Rechte vorbehalten. Frankfurter Rundschau GmbH.

Es ist nicht gestattet, die Inhalte zu vervielfältigen, zu ändern, zu verbreiten, dauerhaft zu speichern oder nachzudrucken. Insbesondere dürfen die Inhalte nicht zum Aufbau einer Datenbank verwendet oder an Dritte weitergegeben werden. Vervielfältigungs- und Nutzungsrechte können unter nutzungsrechte@fr.de oder (069) 7591-2986 erworben werden. Nähere Informationen erhalten Sie unter www.fr-rechte.de.