Spurensuche digital

Big Data bei Polizei und Justiz

JENS RIED
Geboren 1978 in Frankfurt am Main, Koordinator am Center for Management, Technology and Society, Nuremberg Campus of Technology, Friedrich-Alexander-Universität Erlangen-Nürnberg.

Daten bestimmen den Alltag. Immer mehr Geräte, Webseiten, Foren und Social-Media-Anwendungen sammeln immer mehr Daten und vernetzen diese zu immer größeren Sammlungen, die nicht nur ökonomisch von Interesse sind. Diese Datensätze bilden wertvolle Ressourcen, aus denen mit entsprechenden Mitteln sowohl rückblickend Zusammenhänge hergestellt als auch Prognosen künftigen Verhaltens und kommender Entwicklungen mit (zumindest scheinbar) immer größerer Präzision getroffen werden können. Der potenzielle Nutzen für die strategische Unternehmensführung, Marktanalysen und generell die Industrie 4.0 ist ebenso offenkundig wie für die Planung von Wahlkämpfen, die Ermittlung von Risikofaktoren bei der Entstehung von Krankheiten oder die Steuerung von Energieproduktion und -verbrauch auf (inter)nationaler Ebene.

Der in Oxford lehrende italienische Philosoph Luciano Floridi hat für die Lebenswelt, die zunehmend und in nahezu allen Alltagsbereichen von der

Digitalisierung (mit)bestimmt wird, den Begriff der *infosphere* geprägt, um damit zum Ausdruck zu bringen, dass eine Transformation im Gange ist, die nicht nur das individuelle Kommunikationsverhalten verändern wird.[1] Vielmehr wird auch die Art und Weise, wie wir zum Beispiel Lösungen für anstehende Herausforderungen gesellschaftlich aushandeln, zunehmend dem Wandel durch die Digitalisierung unterworfen. Anders ausgedrückt: Unsere Lebenswelt wird zunehmend nicht nur dadurch geprägt, dass wir Daten sammeln und nutzen, sondern auch dadurch, dass wir Daten teils bewusst, teils unbewusst, vor allem aber kontinuierlich liefern und damit eine immer breiter werdende digitale Spur hinterlassen.

Das daraus erwachsende immense Potenzial für die Strafverfolgung ist offensichtlich. Umso bemerkenswerter ist es, dass die Diskussion zu den sich für die Ermittlungsbehörden und die Justiz bietenden Möglichkeiten von Big Data bisher kaum angestoßen wurde. Zwar arbeiten Polizei- und Sicherheitsbehörden in Deutschland bereits seit einigen Jahren mit Methoden, die auf softwaregestützter Analyse von verbundenen Datensammlungen basieren. Die vorhandene wissenschaftliche Literatur zur Anwendung von Big Data in der Strafverfolgung und im Strafprozess ist jedoch erstaunlich dünn gesät. Der instruktive Aufsatz von Christian Rückert ist eine der wenigen Ausnahmen.[2]

„STERNSTUNDE DER KRIMINALISTIK“

Von Interesse sind keineswegs nur solche Daten, die nicht-öffentlich sind, also von den Sicherheitsbehörden zunächst ermittelt und gegebenenfalls beschlagnahmt werden müssen. Relevant sind auch Daten, die sich bereits im Besitz öffentlicher Institutionen befinden oder im Auftrag staatlicher Organe gesammelt werden, jedoch nicht zum Zweck der polizeilichen Ermittlung zusammengetragen worden sind.

Unlängst löste ein Mordfall aus dem Jahr 2016 Diskussionen zu dieser Frage aus: Die Ermittlungen zur Ermordung der Joggerin Carolin G. bei Freiburg hatten Hinweise erbracht, dass der Täter möglicherweise Fernfahrer sein könne. Durch Auswertung von Daten aus dem Mautsystem, deren Verwendbarkeit umstritten war, konnte in Verbindung mit Daten aus dem Mobilfunknetz und einem DNA-Abgleich der Täter in diesem und in mindestens einem weiteren Tötungsdelikt identifiziert werden. Da die Spurenlage zunächst eher schlecht war und sich keine weiterführenden Hinweise ergaben, stellte die Kombination aus Erkenntnissen und den digitalen Daten einen Durchbruch dar. *Die Welt* bezeichnete in ihrer Ausgabe vom 4. Juni 2017 die Lösung des Falls sogar als „Sternstunde der Kriminalistik“.

Als noch relevanter erweist sich die Nutzung öffentlich zugänglicher Informationen. Zum einen wird die Definition von „öffentlich zugänglich“ in der Rechtsprechung oftmals weit gefasst und bezieht sich beispielsweise auch

auf Informationen aus geschlossenen Foren, für die zwar eine Anmeldung erforderlich ist, bei denen aber keine Identitätsprüfung stattfindet. Dies trifft vermutlich auf eine große Zahl entsprechender Kommunikationsanwendungen im Netz zu. Im World Wide Web dürfen Ermittler ohne Beschränkung digitale Spuren verfolgen und nach relevanten Hinweisen suchen, die nicht nur zur Aufklärung, sondern auch zur Verhinderung von Straftaten dienlich sein können. Zum anderen bringt es die digitale Transformation mit sich, dass die Grenzen zwischen der Online- und der Offline-Welt verschwimmen. Das alltägliche Leben wird vermehrt im digitalen Raum dargestellt, kommuniziert und verbreitet. Umgekehrt beeinflussen Impulse aus dem Internet das alltägliche Verhalten. Zugespitzt: Aus der Online-Welt lassen sich zunehmend präzisere und belastbarere Aussagen über Vorgänge in der Offline-Welt ermitteln als aus der Beobachtung der Offline-Welt selbst.

FACEBOOK, FITBIT & CO. ALS ERMITTLUNGSHILFEN

Angesichts der Kontroversen, die bereits die Videoüberwachung öffentlicher Plätze und Gebäude erzeugt, dürfte in den polizeilich genutzten Big Data-gestützten Analysemethoden erhebliches Konfliktpotenzial liegen, doch dazu findet noch keine Debatte statt. Offenbar wird zumindest in der öffentlichen Wahrnehmung die Überwachung des öffentlichen Raumes in der Offline-Welt als problematischer eingeschätzt als die Beobachtung und Auswertung der digitalen Spuren in der Online-Welt. Nicht zuletzt liegt die Ursache dieser scheinbaren Diskrepanz vermutlich darin, dass soziale Medien für einen Zweck genutzt werden, den viele individuell als wichtig empfinden. Anders als bei der Überwachung des realen öffentlichen Raums, die keinen unmittelbaren persönlichen Nutzen erbringt, ist der öffentliche virtuelle Raum nicht nur für die Kommunikation wichtig, sondern dient auch explizit der Verbreitung von Informationen über die eigene Person und steht im Zusammenhang mit der als *Self-Tracking* bezeichneten Aufzeichnung und Auswertung der eigenen Aktivitäten.

Wie relevant diese neuen Möglichkeiten für Polizei- und Justizarbeit werden könnten, lässt sich anhand eines Falls aus den USA illustrieren: Connie Dabate wurde 2015 in ihrem Haus in Ellington (Connecticut) erschossen aufgefunden; ihr Mann Richard war an einen Stuhl gefesselt, aber unverletzt. Er sagte aus, er habe einen Einbrecher überrascht, als er gegen 09.00 Uhr nach Hause gekommen sei. Der Einbrecher habe seine Frau erschossen und ihn fixiert. Die Polizei rekonstruierte die digitale Spur des Falls. Eine entscheidende Rolle spielten dabei Connie Dabates Facebook-Aktivitäten sowie vor allem die Informationen aus ihrer FitBit-Uhr. Es handelt sich dabei um ein sogenanntes *smart device,* das Aktivitäten misst, Informationen

speichert, auswertet und kommuniziert. Connie Dabate trug am fraglichen Vormittag diese Uhr, und die Aufzeichnungen belegten, dass sie sich zuletzt um 10.05 Uhr und nicht etwa, wie von ihrem Ehemann angegeben, gegen 09.00 Uhr bewegt hatte.

Belastbare Beweise liefern die aus einem *smart device* herausgelesenen Daten möglicherweise nicht, aber robuste Indizien. Im Fall Dabate belegen die aufgezeichneten Daten zum Bewegungsprofil des Opfers immerhin, dass die Darstellung des Ehemanns nicht stimmen kann. Ob seine Angaben fragwürdig sind, weil er einem Irrtum erlegen ist, er die zeitliche Abfolge der Ereignisse beziehungsweise ihre Dauer nicht korrekt wiedergeben kann oder weil er seine Täterschaft zu verschleiern sucht, können weder Facebook noch die FitBit nachweisen. Die Notwendigkeit weiterer Ermittlungen kann dagegen durch die Aufzeichnung des Gerätes klar begründet werden. Diese Anhaltspunkte hätte es ohne die Auswertung der Aufzeichnungen wahrscheinlich nicht gegeben. Gleiches gilt für die Anklage und den noch laufenden Prozess gegen Richard Dabate wegen des Mordes an seiner Frau.

WIRD DER „MINORITY REPORT“ WIRKLICHKEIT?

Der offenkundige Nutzen von Big Data für die Ermittlungsarbeit der Sicherheitsbehörden weckt natürlicherweise Begehrlichkeiten nach Zugang zu möglichst umfangreichen Datensammlungen und entsprechender Ausstattung mit Hard- und Software, um das stetig anwachsende Datenkonglomerat sichern, ordnen und auswerten zu können. Besonders verlockend ist dabei die Aussicht, mithilfe dieser Methoden nicht nur eine effektivere Strafverfolgung, sondern eine neue Dimension der Kriminalitäts- und nicht zuletzt auch der Terrorprävention zu erreichen.

Unter dem Stichwort „predictive policing“ werden Methoden zusammengefasst, die auf der Grundlage spezieller Datenanalyseverfahren künftige Straftaten verhindern sollen, indem sowohl Orte als auch Personen identifiziert werden, die mit hoher Wahrscheinlichkeit zum Schauplatz eines Verbrechens beziehungsweise zum Täter oder Opfer werden könnten.[3] Was Philip K. Dick in seiner 1956 erschienenen und 2002 verfilmten Kurzgeschichte *Minority Report* als Ergebnis übernatürlicher Begabungen konzipierte, rückt mit Big Data scheinbar in Reichweite einer technischen Realisierung. Welche Daten allerdings auf welche Weise in ein solches System eingespeist werden sollen, mit welchen Algorithmen die Systematisierung und Auswertung vorgenommen werden soll und – vor allem – welche Konsequenzen aus den Ergebnissen gezogen werden können, ist derzeit noch vollkommen offen beziehungsweise umstritten.

Nicht nur Datenschützer sehen in *predictive policing* erhebliche Probleme, zumal die Zuverlässigkeit der Vorhersagen unklar ist. Dennoch handelt es sich keineswegs um eine theoretische Fiktion. An verschiedenen Stellen in Deutschland wurden entsprechende Verfahren bereits erprobt. Der Freistaat Bayern verwendet beispielsweise seit 2014 in Nürnberg das System PRECOBS *(Pre Crime Observation System)*. Das Programm zielt darauf ab, die zeitnahe Wiederholung eines Delikts aus derselben Deliktsgruppe in einem begrenzten geografischen Raum zu prognostizieren. Dabei werden die Daten derzeit anonymisiert erhoben und ausgewertet, sodass niemand befürchten muss, zu Hause oder bei der Arbeit von der Polizei aufgesucht und wegen eines von ihm oder ihr künftig zu begehenden Verbrechens vorsorglich vernommen oder gar inhaftiert zu werden. Wie sicher und vor allem wie effektiv das System arbeitet, bedarf derzeit noch einer genauen Beobachtung und Auswertung.

Die unter dem Schlagwort „Big Data" zusammengefassten Prozesse und Phänomene sind eine gesellschaftliche Realität, die auch die Art und die Form der Polizei- und Justizarbeit einem Wandel unterwerfen wird. Derzeit ist jedoch sowohl die fachwissenschaftliche als auch die öffentliche Debatte recht überschaubar. Gerade um die Potenziale, die in den zusammenfassend als *smart policing* zu bezeichnenden Entwicklungen liegen, unter angemessener Beachtung der Herausforderungen zu realisieren, bedarf es allerdings einer intensiveren Befassung und auch Auseinandersetzung mit den tatsächlichen Möglichkeiten. An einigen Stellen haben deutsche Behörden bereits erste Erfahrungen und Erkenntnisse gesammelt, die noch der Reflexion und Diskussion harren. Es wäre wünschenswert, wenn mehr Impulse vonseiten der Rechts- und Sicherheitspolitik die Debatte voranbringen würden, damit der anrollende Zug mehr Geschwindigkeit aufnimmt.

[1] Vgl. Luciano Floridi: Die 4. Revolution. Wie die Infosphäre unser Leben verändert, Berlin 2015.

[2] Vgl. Christian Rückert: „Zwischen Online-Streife und Online-(Raster-)Fahndung. Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren", in: Zeitschrift für die gesamte Strafrechtswissenschaft (in Druck).

[3] Zur Übersicht siehe beispielsweise Christina Merz: Predictive Policing. Polizeiliche Strafverfolgung in Zeiten von Big Data, Abida Dossier, Januar 2016, www.abida.de/sites/default/files/Dossier_Predictive_Policing.pdf [letzter Zugriff: 19.08.2017].