Der virtuelle Mr. Hyde

Sebastian J. Golla 2019-09-17T08:05:07

Heute vor einem Jahr brannte es in Zelle 143 der JVA Kleve. Darin eingeschlossen war der junge Syrer Amad A., der wenige Tage später seinen Verbrennungen und Vergiftungen erlag. Amad A. war am 6. Juli 2018 von der Polizei in Geldern festgenommen und darauf inhaftiert worden. Die Inhaftierung erfolgte aufgrund eines Haftbefehls, mit dem der Malier Amedy G. gesucht wurde. Amad A. befand sich fälschlicherweise in Haft und kam auf grässliche Weise ums Leben. Wie konnte es dazu kommen?

Ein Untersuchungsausschuss im Landtag NRW ist mit der Aufklärung des Falles befasst. In der Öffentlichkeit werden mehrere Erklärungen diskutiert.

Nach erster offizieller Darstellung beruhte die Inhaftierung auf einer Verwechslung. Die Polizei habe bei einer Datenabfrage zu Amad A. den Datensatz von Amedy G. gefunden und ihn für diesen gehalten. Nordrhein-Westfalens Innenminister Reul verwies bei einer Fragestunde im Landtag NRW im April darauf, dass dies auf einem sogenannten Kreuztreffer im polizeilichen Informationssystem ViVA beruht haben könnte. Ein Kreuztreffer wird angezeigt, wenn Personen gemeinsame persönliche Merkmale aufweisen. Sowohl Amad A. als auch Amedy G. war der Alias „Amed Amed“ zugeordnet. Daher könnte das System bei der Suche nach Amad A. den Datensatz von Amedy G. angezeigt haben.

Diese Darstellung wirkte aus zwei Gründen wenig plausibel. Erstens hätte die Polizei bei einem Kreuztreffer manuell überprüfen müssen, ob der gefundene Datensatz zu Amad A. passte. Die im Informationssystem hinterlegten Fotos und Beschreibungen von Amad A. und Amedy G. zeigten aber keine besonderen Ähnlichkeiten. Auch Protokolle der Abfragen der Informationssysteme stützten diese Darstellung nicht. Auf dieser Grundlage entstand der Verdacht, dass die Polizei die betreffenden Datensätze vorsätzlich verändert haben könnte.

Anfang Mai wurde dann bekannt, dass eine Sachbearbeiterin der Kreispolizei Siegen die Datensätze von Amad A. und Amedy G. bereits am 4. Juli 2018 in dem Informationssystem ViVA zusammengeführt haben soll. Demnach wäre aus den beiden „Datenbankidentitäten“ eine dritte entstanden, der auch der Haftbefehl von Amedy G. zugeordnet wurde.

Es ist nicht Aufgabe dieses Beitrags, zu spekulieren, welcher Erklärungsansatz zutrifft. Fest steht jedoch: In allen diskutierten Szenarien hätten sich gravierende Risiken im Umgang mit polizeilichen Datenbanken realisiert, die am Ende ein Menschenleben kosteten.

Missrepräsentation und Kriminalisierung

Durch die Zuschreibung von Tatsachen oder Wertungen in polizeilichen Informationssystemen können Personen in Verdacht geraten, Straftaten begangen zu haben oder dazu zu neigen. Gewisse Attribute implizieren kriminelle Verhaltensweisen („Gewalttäter“) oder legen solche nahe („wechselt häufig den Aufenthaltsort“). Dies kann zur Kriminalisierung der Betroffenen beitragen. Wenn Personen gesellschaftliche Rollen zugeschrieben werden, kann daraus resultieren, dass sie diese akzeptieren und übernehmen. Dies kann vor allem fatal sein, wenn eine Attribution fehlerhaft erfolgt.

Kritisch zu begleiten sind daher aktuelle Bemühungen, durch die polizeiliche Daten leichter verfügbar und besser verknüpfbar werden sollen. Je schneller und leichter Daten abrufbar sind und je eher sie routinemäßig abgerufen werden, desto schwerer wiegt das bloße Vorhandensein in der polizeilichen Informationsordnung. Die Standardisierung der Speicherung, die rasche Verfügbarkeit und (teil-)automatisierte Verknüpfung von Daten begünstigen, dass Informationen aus ihrem ursprünglichen Zusammenhang gelöst werden. Es wächst die Herausforderung, Relevanz und Kontext von Informationen zu bewerten.

Die dekontextualisierte Speicherung und Verknüpfung von Informationen kann sich unterschiedlich auswirken. Eine Verwechslung ist eine mögliche Folge. Nach der ersten offiziellen Darstellung im Fall Amad A. soll hier die Zuordnung eines Alias ausgereicht haben, um einer Person eine andere Identität und damit einen Haftbefehl zuzuordnen. Schenkt man dieser Darstellung Glauben, so müssten der Polizei bei der Kontextualisierung der bereitgestellten Informationen entweder krasse Fehler unterlaufen oder eine solche Kontextualisierung ganz unterblieben sein.

Derartige Risiken könnten sich mit dem Einsatz raffinierterer Methoden zur Verknüpfung von Informationen durchaus erhöhen. Möglich erscheint sogar, dass in der polizeilichen Informationsordnung durch die automatisierte Zuschreibung von Eigenschaften Abbilder von Persönlichkeiten entstehen, die sich von ihren Vorbildern loslösen – neben einem reellen Dr. Jekyll könnte sozusagen ein virtueller Mr. Hyde entstehen.

Datenschutz als Lösung?

Diesen Risiken ist unter anderem rechtlich zu begegnen. Bisher wird für den Schutz der Betroffenen im Rahmen der polizeilichen Informationsordnung primär das Datenschutzrecht eingesetzt. Die Ziele und die Funktionsweise der polizeilichen Informationsordnung stehen zum Teil im Widerspruch zu den datenschutzrechtlichen Prinzipien der Zweckbindung, Erforderlichkeit und Datensparsamkeit.

Allerdings ist noch grundsätzlicher zweifelhaft, ob das Datenschutzrecht in seiner traditionellen Ausrichtung als individuelles Abwehrrecht ausreichend ist, um die Betroffenen zu schützen. Die Datenverarbeitung in der polizeilichen Informationsordnung ist auf die Breite ausgelegt. Sie ist von einer besonderen Intransparenz gekennzeichnet, die den individuellen Schutz erschwert. Daher

erscheint mit Blick auf die Kriminalisierung und Missrepräsentation ein verstärkter Blick auf strukturelle Aspekte geboten. Dabei sind unter anderem die institutionelle und prozedurale Dimension des Datenschutzes von Bedeutung, die eine wirksame Kontrolle der Datenverarbeitung erfordern.

Auch Vorgaben an die Organisation und Qualität von Daten könnten der falschen Zuschreibung von Attributen und anderen Risiken entgegenwirken. Die Qualität und Richtigkeit von Daten ist bereits jetzt ein datenschutzrechtliches Prinzip. Nach Art. 4 Abs. 1 lit. d Richtlinie (EU) 2016/680 müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Allerdings ist dieser Grundsatz im nationalen Recht bisher nur schwach ausgeprägt.

Die Anforderungen an die Validierung und Kontrolle von Informationen sollten verstärkt werden. So könnten folgenreiche Datenveränderungen wie die Veränderung von Aliasen oder die Zusammenführung von Datensätzen erschwert werden. Zudem sollte der Grundsatz der Datenqualität als Anforderung an die Struktur von Informationssystemen verstanden werden. Zum Teil sind in polizeilichen Informationssystemen Defizite bei der Datenqualität „vorprogrammiert“ – etwa, wenn arabische Namen erfasst werden. Die traditionelle fünfteilige Struktur dieser Namen lässt sich nicht in das systemisch vorgegebene Schema von Vor- und Nachname pressen. Auch die verschiedenen Transkriptionen von Namen – im Falle von Ahmad etwa Ahmed, Achmed und Achmet – können die Systeme nicht abbilden. Dies kann dazu führen, dass die Träger arabischer Namen unter zahlreichen Aliasen in der Informationsordnung geführt werden und die Verwechslungsgefahr sich deutlich erhöht. Diese strukturellen Defizite sind mit Grundanforderungen an die Datenqualität unvereinbar.

Das herkömmliche Datenschutzrecht neigt außerdem in seiner Konzeption als Vorfeldrecht dazu, einfachgesetzlich aufgeweicht zu werden. Dies zeigt sich bei der Anwendung der Befugnisse zur Informationsordnung in den Polizeigesetzen und der Strafprozessordnung. Diese setzen tatbestandlich im Wesentlichen voraus, dass eine Datenverarbeitung für die Erfüllung polizeilicher Aufgaben oder die Zwecke des Strafverfahrens erforderlich ist. Hieraus werden nur geringe Anforderungen für die Speicherung und Weiterverwendungen von Daten abgeleitet.

Zwar ließen sich aus den Kriterien der Erforderlichkeit und Verhältnismäßigkeit auch strengere Voraussetzungen begründen. Um diese Maßstäbe zu konkretisieren, sollte das Datenschutzrecht aber mit weiteren Rechtspositionen aufgeladen werden. Dieses Potenzial besitzt es aufgrund seiner anerkannten instrumentellen Schutzebene. Mit den Worten von *Nikolaus Marsch* zielt das Datenschutzrecht „nicht selbstzweckhaft auf den Schutz von Daten ab“, sondern dient „dem Schutz einer Vielzahl anderer Rechte und Interessen“ (Das europäische Datenschutzgrundrecht, S. 87).

Diskriminierungsschutz und Unschuldsvermutung

So könnte das Datenschutzrecht das von Art. 3 Abs. 3 GG abgedeckte Interesse am Schutz vor Diskriminierung stärker berücksichtigen. In seiner Entscheidung zur

Antiterrordatei erwähnte das Bundesverfassungsgericht den verfassungsrechtlichen Diskriminierungsschutz im Zusammenhang mit der Aufnahme religionsbezogener Merkmale in Datenbanken und begründete diesbezüglich erhöhte Anforderungen. Für die Berücksichtigung entsprechender Daten sei „von Verfassungs wegen eine zurückhaltende Umsetzung geboten“. Dem sei „dadurch Rechnung zu tragen, dass die Aufnahme entsprechender Angaben nicht über eine lediglich identifizierende Bedeutung hinausgeht“. Daraus lässt sich folgern, dass nach Art. 3 Abs. 3 Satz 1 GG geschützte Merkmale ohne besondere Rechtfertigung nicht in Datenbanken vorgehalten werden dürfen, um diese zur Grundlage einer Bewertung zu machen.

Auch die nach Art. 6 Abs. 2 EMRK gewährleistete Unschuldsvermutung kann das Datenschutzrecht aufladen und seine Schutzrichtung konkretisieren. Sie schützt nach dem Bundesverfassungsgericht nicht nur vor Schuldspruch und Strafe, sondern auch vor Nachteilen, die diesen „gleichkommen, denen aber kein rechtsstaatliches prozessordnungsgemäßes Verfahren zur Schuldfeststellung vorausgegangen ist“. Das Gericht sieht die Speicherung personenbezogener Daten aus (abgeschlossenen) Strafverfahren zwar regelmäßig nicht im Konflikt mit der Unschuldsvermutung. So kann die Unschuldsvermutung weder vor Strafverfolgung, noch vor der Speicherung von Daten zur vorbeugenden Verbrechensbekämpfung schützen, wenn es hierfür einen Anlass gibt. Jedoch leitet das Bundesverfassungsgericht aus der Unschuldsvermutung eine Anforderung an die Datenqualität ab, wonach Verdachtsdaten nach einem Freispruch oder einer Verfahrenseinstellung zu überprüfen sind. Berichten der Datenschutzaufsicht zufolge wird dies in der Praxis allerdings nicht immer beherzigt.

Treffender als das Bundesverfassungsgericht greift der Europäische Gerichtshof für Menschenrechte die Risiken der Datenspeicherung auf und berührt dabei ebenfalls das komplizierte Verhältnis von Datenschutz und Unschuldsvermutung. Im Fall *Marper* stellte der EGMR fest, die Speicherung personenbezogener Daten aus Strafverfahren könne nicht mit der Äußerung eines Schuldverdachtes gegenüber der betroffenen Person gleichgesetzt werden. Gleichwohl würde „ihre eigene Wahrnehmung, sie würden nicht als unschuldig behandelt, dadurch verstärkt, dass ihre Daten wie bei verurteilten Straftätern auf unbegrenzte Zeit gespeichert werden, während die solcher Personen, die nie einer Straftat verdächtig waren, vernichtet werden müssen“. Dies benennt das Risiko einer kriminellen Etikettierung direkt.

Interessant ist in diesem Zusammenhang auch der Fall *Khelili*: Eine Frau war über 18 Jahre lang in einer polizeilichen Datenbank als Prostituierte gekennzeichnet gewesen, weil bei ihr verdächtige Visitenkarten aufgefunden worden waren. Die Attribution in der Datenbank legte ein strafbares Verhalten nahe, obwohl Frau Khelili nie verurteilt worden war. Dies sah der Gerichtshof auch angesichts der langen Speicherdauer „insbesondere im Hinblick auf das überragende Prinzip der Unschuldsvermutung“ als Verletzung von Art. 8 EMRK an.

Die potentiell stigmatisierenden Wirkungen einer Datenspeicherung zu Zwecken der Kriminalprävention sollten der Rechtsprechung des EGMR folgend genau berücksichtigt werden. Dies direkt an der Unschuldsvermutung festzumachen ist zwar nicht zwingend, sie bietet aber zumindest einen Anhaltspunkt für die relevanten Risiken.

Aufklärung und Konsequenzen

Der Fall Amad A. wirft ein Schlaglicht auf Risiken der polizeilichen Informationsordnung. Gravierende Defizite beim Umgang mit Daten könnten hier mit ursächlich für den Tod eines jungen Menschen geworden sein. Es ist zu hoffen, dass dem nordrhein-westfälischen Untersuchungsausschuss eine umfassende Aufklärung des Falles gelingen wird, aus der auch Konsequenzen für den Umgang mit Informationssystemen folgen.

Derweil dürften sich die benannten Risiken in vielen Fällen eher im Verborgenen realisieren. Gerade im Zusammenhang mit der aktuellen Neuordnung des polizeilichen Informationswesens verdienen sie mehr Aufmerksamkeit. Um Betroffene zu schützen, bedarf es nicht nur einer Aktualisierung der materiellen datenschutzrechtlichen Vorgaben. Auch eine genaue Analyse der Risiken, eine wirksame Kontrolle sowie technische Schutzmaßnahmen sind unerlässlich.
