Big Data und Datenschutz – ein unauflöslicher Widerspruch?

Zusammenfassung der Keynote von Staatssekretär Martin Jäger zur Herbstkonferenz Datenschutz des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Es liegt vermutlich in der Natur der Sache, dass zwischen einem Staatssekretär, der verantwortlich ist für die Sicherheit und den Bevölkerungsschutz, und den Vertretern des Datenschutzes eine gewisse Reibung besteht. Das wird einer der Gründe sein, warum ich eingeladen wurde hier zu sprechen: Damit wir etwas Reibungshitze miteinander teilen.

Ich weiß sehr wohl, dass Sie als Datenschützer die Belange der Sicherheit sehr ernst nehmen. Sie dürfen umgekehrt versichert sein, dass mir das Grundrecht auf informationelle Selbstbestimmung am Herzen liegt. Sicherheit ermöglicht Freiheit, sie darf die Freiheit aber nicht zur Farce machen. Wo Friedhofsruhe herrscht, da gibt es keine tatsächlich gelebte Freiheit mehr. Die Erfahrung zweier Diktaturen lässt uns in Deutschland in dieser Hinsicht besonders vorsichtig sein.

Über all das brauchen wir hier und heute gar nicht zu diskutieren, sie sind mir so selbstverständlich wie Ihnen. Es gibt dann aber doch ein paar Dinge, über die wir sprechen müssen.

Meine These ist diese: Der Datenschutz - zumindest in Europa - steht vor einem Umbruch. Er ist gemacht nach den Erfahrungen der Vergangenheit. Künftig wird er sich aber neu orientieren müssen: Anstatt sich vorrangig und mit Verve auf den Staat und seine Behörden zu konzentrieren, wird der Datenschutz sich sehr viel intensiver mit der massenhaften Sammlung, Verknüpfung und algorithmenbasierten Auswertung von Daten durch Unternehmen befassen müssen.

Natürlich bin ich mir der Tatsache bewusst, dass der Datenschutz sich im Rechtsgefüge unseres Landes eine überaus starke Position erkämpft hat. Ihre Stimme wird gehört, Ihr Ratschlag zählt – in Politik und Gesellschaft.

Ihren spürbaren Ausdruck findet diese Wirkmacht in der europäischen Datenschutzgrundverordnung, die Ende Mai des kommenden Jahres in Kraft treten wird. Das ist der gesetzliche Rahmen, dem wir alle – Sie wie ich – künftig verpflichtet sind, und es steht außer Frage, dass wir geltendes Recht einzuhalten haben. Selbstverständlich auch dort, wo ich persönlich in der Gesetzgebung lieber andere Akzente gesetzten hätte. Das Recht bindet, ohne Wenn und Aber. So sind die Spielregeln im demokratischen Rechtsstaat.

Trotzdem müssen wir uns die Frage stellen, ob dieses Recht den Anforderungen unserer Gegenwart genügt. Sie als Datenschützer haben hart darum gerungen, dass wir das heute etablierte Schutzniveau erreichen konnten. Das alles stößt selbstredend auch auf meine Zustimmung. Und nicht zufällig geht es in der Auseinandersetzung mit den Populisten jedweder Couleur immer auch um die Bewahrung und die Verteidigung dieses Konsenses.

Ich fürchte nur, mit reiner Beschwörung und immer weiter vorangetriebener Verfeinerung des Erreichten ist es nicht länger getan. Dies käme einem Rückzug in die Wagenburg gleich. Für den Datenschutz - ich habe es angedeutet - sehe ich zwei Aspekte, mit denen wir uns stärker als bisher zu beschäftigen haben.

Erstens: Wir sind mit einer neuen Sicherheitsproblematik konfrontiert. Der Datenschutz muss sein Verhältnis zum Staat überdenken und besser begreifen lernen, dass es in Zeiten, wo die liberale Demokratie weltweit unter Beschuss gerät, ohne einen handlungsfähigen Staat nicht geht. Nur mit einem starken Staat werden wir unsere Freiheit bewahren.

Zweitens: Der Datenschutz sollte wissen, dass es auf Dauer keinen Sinn ergibt, sich vorwiegend an staatlichen Organen, insbesondere den Sicherheitsbehörden abzuarbeiten. Künftig sollten die Unternehmen stärker im Fokus stehen – in ihrer

täglichen Rechtsanwendung, auch ihrer Unsicherheit im Umgang mit dem neuen Datenschutzrecht, aber eben auch im Hinblick auf jene Unternehmen, die ihr Geschäftsmodell vorrangig auf die massenhafte Sammlung und Strukturierung von Daten ausrichten.

Seien wir ehrlich miteinander: Der Datenschutz ist vielleicht auch deshalb so sehr auf das Handeln staatlicher Behörden fixiert, weil „wir vom Staat“ ja immer druckempfindlich sind und in der Regel schnell parieren, wenn Kritik seitens der Datenschützer kommt. Unternehmen dagegen, vor allem wenn sie transnational agieren und ganz unterschiedlichen Rechtsprechungen unterliegen, sind deutlich schwerer am Wickel zu packen. Diese international operierenden Unternehmen sind für den Datenschutz in Europa deutlich schwierigere Gegner als nationale, staatliche Behörden, die lückenlos der demokratischen Kontrolle und der Rechtsaufsicht der nationalen Verwaltungsgerichte unterliegen.

Es ist nur so: Die Wirklichkeit fragt uns nicht, was wir uns wünschen. Wir müssen schon selber wissen, wohin wir wollen und entsprechend handeln. Sonst gewinnt am Ende die Macht des Faktischen. Egal wie kontrafaktisch wir denken. Worüber wir gemeinsam und ohne Scheuklappen nachdenken müssen, ist die Frage, wie es unter sich rasant verändernden Bedingungen gelingen kann, Freiheit und Sicherheit und ihr Verhältnis zueinander weiter zu denken.

Lassen Sie mich ein paar konkrete Anmerkungen zur Beziehung von Datenschutz und Sicherheitsbehörden machen.

Ich beginne mit einem Sachverhalt, der uns hier im Land sehr beschäftigt hat. Nach einem Mord, begangen an einer jungen Studentin in Freiburg, haben wir uns die Gruppe der minderjährigen unbegleiteten Flüchtlinge genauer angeschaut. Denn der Freiburger Tatverdächtige ist ein afghanischer Asylbewerber. Und wie sich dabei herausstellt: minderjährig ist der Tatverdächtige jedenfalls nicht. Obwohl er genau unter dieser Flagge gesegelt ist.

Mehr noch: Wir haben festgestellt, gut ein Drittel bis die Hälfte der sog. UMAs wurde gar nicht erst erkennungsdienstlich behandelt, als sie nach Deutschland kamen.

Das geht natürlich nicht. Wir müssen wissen, wer bei uns ist. Wir müssen auch wissen, ob er andernorts schon straffällig geworden ist. Also haben wir beschlossen, alle unbegleiteten Minderjährigen zu überprüfen.

Dass dies möglich wurde, haben wir auch der pragmatischen Zusammenarbeit mit dem Datenschutzbeauftragten zu verdanken. Das würdige ich ausdrücklich.

Das Ergebnis überzeugt. Unter anderem haben wir einen Fall ans Licht gebracht, wo ein angeblicher UMA sich als ein Mann von 37 Jahren herausgestellt hat. Man glaubt es nicht. Und doch ist es wahr.

Aber jetzt kommt der Wehmutstropfen: Etwa zehn Prozent der eingeladenen UMAs sind unserer Bitte zur Vorstellung nicht nachgekommen. Nun liegt es in der Natur der Sache, dass gerade diese Gruppe die für uns potentiell interessanteste ist. Nur kann ich die Liste dieser Leute leider nicht abrufen, weil sie gelöscht wurde, wie es der Vorgabe durch den Landesdatenschutz entspricht.

Ein weiteres Beispiel: Die Zahl der islamistischen Gefährder steigt sprunghaft. Nicht annähernd so dynamisch wachsen unsere Ressourcen, um solche Gefährder im Blick zu behalten. Um einen dieser Gefährder rund um die Uhr zu beobachten, brauchen wir bis zu 30 Polizisten, in manchen Fällen mehr als doppelt so viele.

Sie können sich leicht vorstellen, was das in der Realität bedeutet. Mit der klassischen Observierung allein bekommen wir das nicht mehr hin. Wir brauchen deshalb Instrumente wie die Quellen-TKÜ oder die Online-Durchsuchung samt GPS-Standortbestimmung.

Ich will diese Instrumente hier nicht zum Allheilmittel erklären. Im Fall von Anis Amri, dem Attentäter von Berlin, haperte es vor allem an der lückenlosen Zusammenarbeit der beteiligten Behörden, das ist mir wohl bewusst.

Trotzdem brauchen wir Instrumente wie Quellen-TKÜ und Online-Durchsuchung – und zwar dringend! Alles selbstverständlich mit Richtervorbehalt und vernünftigen Protokollierungs- und Benachrichtigungspflichten. Wir werden schon bald über die Konfiguration und den konkreten Einsatz solcher Software sprechen müssen.

Unlängst hatte ich anlässlich eines Interviews, das wir gemeinsam geführt haben, Gelegenheit, mich länger mit Gerhart Baum zu unterhalten. Wir sind uns nicht in allem und jedem einig geworden – etwa bei den Vorratsdaten – aber ich habe viel gelernt von Gerhart Baum. Ich habe mir auch seinen Hinweis gemerkt, dass heute niemand wissen kann, was einmal in der Zukunft mit gespeicherten Daten geschieht. Deshalb sei es besser, so wenige Daten wie möglich und nötig aufzubewahren. Ich stimme zu.

Gerhart Baum, der ja in politischer Verantwortung während der RAF-Jahre stand, hat mir gegenüber aber auch bekräftigt, dass der Staat und die freie Gesellschaft sich mit den ihr zu Gebote stehenden und rechtlich verfügbaren Mitteln wehren müssen, wenn sie angegriffen werden.

Lassen Sie mich einige Bemerkungen ergänzen zum zweiten Aspekt, den ich vorher angerissen habe: Dem Umgang mit Big Data und den transnational agierenden Unternehmen. Wie gehen wir um mit Unternehmen und Dienstleistern, die ihr Geschäftsmodell auf Big Data stützen?

Durch Big Data-Anwendungen erwachsen wirtschaftliche Möglichkeiten, dort wo mit personenbezogenen Daten gearbeitet wird, entstehen mögliche Gefahren für das informationelle Selbstbestimmungsrecht der Bürger. Darauf müssen wir reagieren.

Diese Risiken lassen sich auf unterschiedliche Weise beherrschen. Etwa, indem man die erhobenen Daten vor der Analyse anonymisiert oder den Personenbezug zumindest durch Pseudonymisierung erheblich reduziert.

Noch sind wir in Deutschland von diesen Entwicklungen vermutlich nicht so stark betroffen wie anderswo auf der Welt, und es ist auch nicht so, als ob wir keine rechtliche Handhabe hätten. Wir sind dennoch gut beraten, uns politisch vertiefter mit dieser Problematik auseinander zu setzen.

Ich befürchte, eine Offenlegung des Algorithmen-Quelltextes wäre nicht zielführend. Dies würde berechtigte Geschäftsgeheimnisse der Unternehmen verletzen und den durchschnittlichen Verbraucher schlicht überfordern. Wie also mit solchen Fragen in der Praxis umgehen?

Ein Beispiel aus Stuttgart: Ein Industriekonsortium beschäftigt sich mit der Entwicklung einer App-basierten Verkehrslenkung. Basis hierfür ist eine neue Datenplattform, die alle relevanten Informationen der regionalen Partner zur Verkehrssteuerung zusammenbringt. Am Ende soll ein Mobilitätsassistent für die Metropolregion Stuttgart stehen, der mit Echtzeitdaten aus einer Big Data-Plattform versorgt wird.

Mit Blick auf personenbezogene Daten wird es dann so sein, dass lediglich Nutzer, die auch Tickets über die App bestellen möchten, ihre persönlichen Daten im verschlüsselten Abrechnungssystem hinterlegen müssen. Zwischen den Anwendungen wird dann nur eine anonyme Nutzer-ID verwendet, um einen hohen Datenschutz zu gewährleisten. Dies, zusammen mit dem Grundsatz der Datensparsamkeit, wird zudem während des gesamten Projekts durch die Einbeziehung des Landesdatenschutzbeauftragten sichergestellt.

Ein anderes Beispiel ist das autonome Fahren. Auch dies in der Praxis eine hochkomplexe Big Data-Anwendung. Die Ironie dabei: Obwohl die Beteiligung des Menschen am Fahren entbehrlich wird, werden zwangsläufig viele Daten über die

mitfahrenden Menschen gesammelt. Wer fährt wann wohin? Wie lange bleibt er dort? Fährt er alleine oder zu zweit?

Wie gehen wir mit diesen Informationen um? Klar ist, die Unternehmen müssen jederzeit in der Lage sein, den Nachweis zu erbringen, dass sie die Verarbeitung personenbezogener Daten datenschutzrechtskonform ausüben.

Konkret heißt dies: Überall, wo Big Data eingesetzt wird, muss vorher im Rahmen einer Datenschutzfolgeabschätzung das Risiko analysiert und anschließend – auch mit Hilfe der Datenschutzbeauftragten – festgelegt werden, welche Maßnahmen geeignet sind, um den Datenschutz zu gewährleisten.

Eine Pseudonymisierung wird hier nur selten als ausreichend angesehen werden, da immer die Gefahr besteht, dass bei entsprechendem Aufwand eine Re-Identifizierung möglich ist. Anzustreben ist daher möglichst eine Anonymisierung, so dass die Daten nicht mehr einer bestimmten Person zugeordnet werden können. Hier gibt es verschiedene Ansätze - Sie kennen sich hier besser aus als ich - doch wir alle miteinander wissen, dass es noch einigen Forschungsbedarf gibt, damit wir eine solche Anonymisierung wirksam gewährleisten können.

Generell gilt sicher: Je sensibler die personenbezogenen Daten, desto strenger müssen die Vorkehrungen sein. Niemand sollte, außer mit seiner Einwilligung oder aufgrund eines Gesetzes, automatisch als Ergebnis einer Datenanalyse einer Entscheidung unterworfen werden.

Solche Schranken müssen für uns der Handlungsmaßstab sein - und nicht etwa die Größe oder Marktkapitalisierung der in Frage stehenden Unternehmen.

Dank Big Data kennen US-Internethändler wie Amazon und eBay ihre Kunden in Stadt und Land mittlerweile ähnlich gut, wenn nicht noch besser, als die vielen kleinen und mittelständischen Unternehmen, die ja gerade von dieser Kundennähe leben. In den USA haben Unternehmen den Wettbewerbsvorteil,

dass sie für Big-Data-Anwendungen nur die dort geltenden weniger strengen *Privacy*-Anforderungen beachten müssen.

In Europa konnte unter der seit 1995 geltenden Datenschutz-Richtlinie ein Standort mit den relativ geringsten Datenschutzanforderungen gewählt werden. So wählten Facebook, Google, LinkedIn, Apple und Twitter Irland als ihren Sitz innerhalb der EU. Es ist daher richtig, dass wir in der EU mit der Datenschutz-Grundverordnung einen einheitlichen Rahmen schaffen. Entsprechend müssen wir die nationalen Regeln anpassen.

Das Bundesdatenschutzgesetz liegt bereits in neuer Fassung vor. Die Länder, darunter auch wir, arbeiten an der Novellierung ihrer Landesdatenschutzgesetze, um die europäischen Vorgaben auch für den öffentlichen Bereich der Länder umzusetzen.

Selbstverständlich berührt diese Problematik am Ende auch wieder die Arbeit der Sicherheitsbehörden. Wir werden im kommenden Frühjahr deshalb auch unser Polizeirecht an die europäischen Vorgaben anpassen. Wir werden als Landespolizei aber auch selbst in die Nutzung von Algorithmen einsteigen. Erste Versuche des *Predictive Policing* haben gemischte Ergebnisse zutage gebracht. Auf dem Feld der sog. intelligenten Videoüberwachung wollen wir - gemeinsam mit dem Landesdatenschutzbeauftragten - in die pilotierte Erprobung einsteigen und Erfahrungen sammeln. Darüber werden wir dann gerne berichten.