Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Die Anonymisierung im Datenschutzrecht“

beim „DatenTag“ der Stiftung Datenschutz

Bonn, den 7. Dezember 2022

Es gilt das gesprochene Wort

Sehr geehrter Herr Richter,
meine Damen und Herren,
liebe Kolleginnen und Kollegen,

ich freue mich, heute Teil dieser Veranstaltung in Bonn zu sein. Wir sind zur Frage der Anonymisierung von personenbezogenen Daten zusammengekommen. Was nüchtern wirkt, ist inhaltlich sehr viel mehr: Denn gerade heute, gerade bei diesem Thema, geht es darum, mit Ihnen gemeinsam zu diskutieren, wie wir Innovationen mit und durch Datenschutz ermöglichen können.

Wie sieht also unsere Datenstrategie aus, wie die Zukunft, in der wir in einer zunehmend digitalisierten Welt leben wollen?

Datenschutz setzt klare Leitplanken für die ökonomische, politische oder wissenschaftliche Verwertung personenbezogener Daten. Anonymisierung schafft Freiräume für Forschung, Wertschöpfung und Innovationen. Damit ist sie ein mächtiges Instrument.

Das Wesen der Anonymisierung besteht vereinfacht darin, den Personenbezug von Daten aufzuheben. Mit dem Einsatz von Anonymisierungstechniken soll erreicht werden, dass die betroffene Person nicht mehr identifiziert werden kann. Intelligente Anonymisierung versucht gleichzeitig aber, den maximalen Erklärungsgehalt von Daten zu bewahren. Nutzen und Werthaltigkeit von Daten auf der einen, Schutz der Menschen auf der anderen Seite.

Gute Anonymisierung muss beiden Zielen gerecht werden. Und wir alle wissen, dass dies ein wenig wie der Versuch nach der Quadratur des Kreises klingt.

Ich wurde gebeten, die datenschutzrechtliche Position in diese Diskussion mit einzubringen. Das mache ich herzlich gerne. Als Datenschützer ist Anonymisierung und die Möglichkeit zum anonymen Agieren auf ganz unterschiedlichen Ebenen relevant.

Lassen Sie mich hier zunächst ganz allgemein beginnen:

Natürlich gibt es in unserer Lebenswirklichkeit unterschiedliche Situationen, in denen uns die Identität des menschlichen „Gegenübers“ wichtig ist. Das war schon immer in der analogen Welt so und gilt natürlich auch im „digitalen“ Raum. Das mag auf elektronischen Handelsplattformen der Fall sein, wenn es darum geht, seinen Vertragspartner zu kennen. Das mag aber auch der Fall sein, wenn es darum geht, kriminelles Verhalten im Internet aufzuklären. Etwa bei Hasskommentaren in sozialen Netzwerken oder bei Geldwäsche.

Genauso gut gibt es aber Situationen, in denen uns die Identität des Gegenübers nicht wichtig sein sollte – nicht wichtig sein darf. Denn Anonymität ist ein hohes Gut. Anonymität ist aktiver Grundrechtsschutz.

Was meine ich damit?

Anonymität ist Freiheit. Nach meiner festen Überzeugung ist Anonymität ein Grundprinzip des freien Internets. Das Internet kann ein mächtiges Instrument zur Sicherung der Meinungspluralität und freien Meinungsäußerung sein. Denken Sie daran, welche Rolle das Internet zunächst für die Umbrüche in der arabischen Welt spielte. Aber auch, welche Bedeutung dem freien – anonymen Internet – ganz aktuell im Ukrainekrieg oder der Revolution im Iran zukommt. Neue Medien und das Internet haben eine entscheidende Funktion, wenn es darum geht, Informationen und Bilder zu verbreiten und Menschen zu erreichen.

Das Beispiel zeigt, was für ein herausragendes Gut das freie, offene und eben aber auch grundsätzlich anonyme Internet ist. Und es zeigt auch, warum es wichtig ist, diese Freiheit immer wieder aufs Neue zu verteidigen. Auch vor diesem Hintergrund hat der EuGH jüngst wieder einmal der anlasslosen, unterschiedslosen Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten eine klare Absage erteilt.

Denn was nicht sein darf, ist das diffuse Gefühl eines jeden Einzelnen, allgegenwärtig beobachtet zu sein und bewertet zu werden, ob durch staatliche Stellen oder private Konzerne. Diese Freiheit müssen wir bei allen technischen Entwicklungen von Anfang an berücksichtigen und dafür Sorge tragen, sie zu bewahren bzw. wieder zu erlangen.

Als Datenschützer kann ich auf das grundlegende Volkszählungs-Urteil des BVerfG verweisen. Das Recht auf informationelle Selbstbestimmung umfasst „die Befugnis eines jeden Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“ Jeder sollte also selbst bestimmen können, mit welchen Inhalten er in Beziehung zu seiner Umwelt treten will und wie die eigene Persönlichkeit unter Wahrung von Privatheit entfalten will. Diese Linie hat das Bundesverfassungsgericht in den darauffolgenden vier Jahrzehnten immer wieder betont und detailliert ausgestaltet. Sie ist aktueller als je zuvor.

Und Anonymität ist hierbei ein gewichtiger Garant.

Dies ist eine Facette der Anonymität, die heute nicht unmittelbar im Fokus der Veranstaltung steht, mir aber besonders am Herzen liegt.

Wie Sie wissen, bekenne ich mich dazu, Datenschutz als Innovationsförderer zu verstehen. Eine – wie ich weiß – nicht ganz unumstrittene Position. Aber auch an dieser Stelle möchte ich dafür werben:

Denn Anonymität ist ein „Möglich-Macher“. Auf diese „Enabler-Funktion“ hatte ich eingangs bereits kurz hingewiesen. Die Frage ist doch, wie wir es schaffen, Mehrwerte aus personenbezogenen Daten zu ziehen, ohne datenschutzrechtliche Risiken für Betroffene zu generieren.

Anwendungsfälle gibt es unzählige, in allen Bereichen unseres gesellschaftlichen und wirtschaftlichen Lebens. Augenfällig sind zahlreiche Beispiele aus dem Bereich der medizinischen Forschung. Für viele Forschungsprojekte – etwa das Trainieren von Künstlicher Intelligenz – ist die Analyse von Datensätzen ausreichend, deren abstrakter Gehalt erhalten bleibt, deren Personenbezug jedoch aufgehoben wird. Gleiches gilt für zahlreiche Geschäftsmodelle.

Trotz ihrer hohen praktischen Bedeutung ist die Anonymisierung gesetzlich aber leider nur rudimentär geregelt. In der DSGVO werden anonyme und anonymisierte Daten nur in einem Erwägungsgrund genannt.[1] Die Grundsätze des Datenschutzes sollen nicht für anonyme Informationen gelten, „d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“. Weitere Bestimmungen hierzu enthält die DSGVO nicht.

Rechtlich wird also anerkannt, dass die Grundsätze des Datenschutzes bei einer hinreichenden Anonymisierung nicht gelten.

Wann aber eine Anonymisierung als hinreichend angesehen werden kann, darüber gibt die DSGVO keine abschließende Auskunft.

[1] Erwägungsgrund 26 Sätze 4 und 5.

So wird im gleichen Erwägungsgrund der DSGVO nur festgehalten, dass bei einer möglichen Identifizierung „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren“.2 Hierbei wiederum „sollten alle objektiven Faktoren, wie Kosten der Identifizierung und der erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind“.[3]

In meinem Haus beschäftigen wir uns seit Jahren mit den rechtlichen und technischen Fragen der Anonymisierung. Bereits Anfang 2020 haben wir ein öffentliches Konsultationsverfahren zur Anonymisierung initiiert, um einen Beitrag zu mehr Rechtsklarheit zu leisten.

Im Fokus stand hier die Telekommunikationsbranche. Denn gerade in dieser fallen zahlreiche Verkehrs- und Standortdaten an. So wundert es nicht, dass Telekommunikationsanbieter über neue datengetriebene Dienste nachdenken, um Verkehrsflüsse zu analysieren, den optimalen Standort für ein neues Einkaufscenter zu bestimmen oder die Kundenutzung bestimmter Telefontarife und deren Wirtschaftlichkeit genauer zu bewerten.

[2] Erwägungsgrund 26 Satz 3.

[3] Erwägungsgrund 26 Satz 4.

Das Ergebnispapier zum Konsultationsverfahrens hat insbesondere zu einigen Rechtsfragen mehr Klarheit gebracht. Lassen Sie mich drei konkrete Aspekte nennen:

1. Jede Anonymisierung stellt eine Verarbeitung personenbezogener Daten dar und bedarf deshalb einer Rechtsgrundlage.

2. Die Verpflichtung zur Löschung von personenbezogenen Daten ist durch Anonymisierung erfüllbar.

3. Im Rahmen der Transparenzpflichten hat der Verantwortliche den Betroffenen die Zwecke und die Rechtsgrundlage der Anonymisierung mitzuteilen.

Weiterhin ungeklärt bleiben aber zahlreiche technische Fragen der Anonymisierung. Bei dem technischen Vorgang des Anonymisierens verdient die Validität des eingesetzten Anonymisierungsverfahrens ein ganz besonderes Augenmerk. Unser heutiger Gastgeber Frederick Richter hat in einem Aufsatz in ein schönes Bild gebracht: „Beim Durchschreiten des verheißungsvollen „Tores in die Datenfreiheit“ können einige Dinge schiefgehen.“[4] Das ist richtig. Man könnte auch sagen: Die Validität der Anonymisierung bedarf tatsächlich einer kontinuierlichen Überprüfung durch den Verantwortlichen.

[4] Richter, Macht die Anonymisierung attraktiv, PinG 05/20, 181 f.

Denn die aus einer misslungenen Anonymisierung resultierenden Risiken für Betroffene sind massiv: In den eingangs genannten Beispielen können etwa Bewegungsprofile von Mobilfunknutzern entstehen oder – und auch hierfür braucht es in der heutigen Welt wenig Fantasie – gar die Demaskierung eines Regimekritikers drohen.

Auch in diesem Punkt kommt es aus meiner Sicht aber natürlich gleichwohl auf die Balance an. Eine absolute Anonymisierung derart, dass die Wiederherstellung des Personenbezugs für niemanden möglich ist, ist oft nicht realisierbar. Sie ist im Regelfall datenschutzrechtlich auch nicht gefordert. Ausreichend ist regelmäßig, dass der Personenbezug derart aufgehoben wird, dass eine Re-Identifizierung praktisch nicht durchführbar ist.

Die robuste – und damit datenschutzadäquate – Anonymisierung bleibt aber eine echte Herausforderung für den jeweiligen Verantwortlichen. Wann ist von einer belastbaren Anonymisierung auszugehen, wann nicht? Hier fehlt es an Orientierung, obwohl diese für die Praxis wichtig wäre. Gerade deshalb sind Leitlinien wertvoll.

Auch auf europäischer Ebene wird derzeit an solchen neuen Leitlinien für Anonymisierung gearbeitet. Darin werden den Verantwortlichen drei wichtige Kriterien genannt, die einen Hinweis auf einen verbleibenden Personenbezug geben:

1. „Singling Out“ meint das Vorhandensein von eindeutigen Daten, die zu einer individuellen Person gehören.

2. „Linkage“ beschreibt die Möglichkeit, einen Eintrag mit einem zur gleichen Person gehörenden weiteren Eintrag aus einem anderen Datensatz zu verbinden.

3. „Inference“ ist die Möglichkeit, aus den Daten Informationen über eine Person herzuleiten, beispielsweise die Tatsache, dass personenbezogen Daten dieser Person in die Anonymisierung mit eingeflossen sind.

Das Vorhandensein dieser Kriterien lässt nicht zwingend darauf schließen, dass die untersuchten Daten nicht anonym sind. Aber die Vermeidung dieser Eigenschaften ist unbedingt zu empfehlen und eine wertvolle „best practice“.

Und wir alle benötigen diese „best practices“, um die genannten Innovationspotenziale zu heben. Und hier komme ich auf meine Grundthese zurück: Der Datenschutz ist kein Hemmnis. Das Gegenteil ist der Fall. Wenn von Daten aufgrund einer Anonymisierung keine Risiken für Rechte und Freiheiten natürlicher Personen mehr ausgehen, spricht nichts dagegen, mit diesen Informationen Wertschöpfung und Mehrwerte zu generieren. Als Datenschützer unterstütze ich diese Datennutzung ausdrücklich. Denn sie ist ein echter Erfolgsfaktor für eine Datenökonomie, die den Menschen im Fokus hat und Grundrechte wahrt. Sie ist damit Basis einer klugen Datenstrategie.

Besonders begrüßen möchte ich daher auch den Vorstoß Ihres Projektes zur Schaffung von Grundlagen für Verhaltensregeln zur Anonymisierung. Verhaltensregeln nach Art. 40 DSGVO sind ein wertvolles und bislang unterschätztes Mittel, um Unsicherheiten abzubauen und Datennutzung erfolgreich zu gestalten.

In diesem Sinne bin ich sehr gespannt auf die Ergebnisse ihrer Projektvorstellung zur Anonymisierung von Daten.

Ich danke Ihnen für Ihre Aufmerksamkeit.