Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Trau, schau wem – der Westen braucht einen gemeinsamen Datenraum“

Ringvorlesung
„Lasst uns reden... über Ethik und Nachhaltigkeit in der digitalen Welt“
am Zentrum für Ethik und Verantwortung der
Hochschule Bonn-Rhein-Sieg

29. November 2021

Es gilt das gesprochene Wort

Sehr geehrte Damen und Herren,

auch ich freue mich, Sie im Rahmen der Ringvorlesung „Lasst uns reden... über Ethik und Nachhaltigkeit in der digitalen Welt“ begrüßen zu können. Das Thema der heutigen Veranstaltung lautet „Trau, schau wem – der Westen braucht einen gemeinsamen Datenraum“.

Wobei ich – um berechtigte Nachfragen im Vorfeld zu beantworten – den Westen dabei eher als Synonym für demokratisch verfasste, liberal gesinnte Staaten verstehe. Vor der Diskussion dieses datenschutzpolitisch aktuellen Themas heute hier in der Hochschule Bonn-Rhein-Sieg lassen Sie mich aus meiner Sicht als Bundesdatenschutzbeauftragter zunächst skizzieren, warum sich die Forderung nach einem gemeinsamen Datenraum stellt und wie die hierfür notwendigen Schritte aussehen könnten.

I. Problemaufriss

Noch nie in der Geschichte der Menschheit war die weltweite Vernetzung größer als heute. Ob Rechnungslegung, Personalmanagement, Fernwartung oder Cloud-Computing: Im Zuge der Globalisierung und der Digitalisierung lagern nicht nur große Konzerne, sondern auch immer mehr kleine und mittlere Unternehmen Geschäftsprozesse weltweit aus – sei es, um Kosten zu sparen oder aus Mangel an vergleichbaren heimischen Angeboten.

Auf den globalen Märkten werden Waren und Dienstleistungen gehandelt, Investitionen getätigt und Technologien übertragen. Und dabei wird notwendigerweise eine Vielzahl von Informationen ausgetauscht.

Prognosen zufolge wird sich das weltweite Datenvolumen Ende 2022 seit 2018 verdoppelt haben und zwischen den Jahren 2022 und 2025 dann noch einmal verdoppeln: Es werden mehr Informationen erzeugt, gesammelt und genutzt als je zuvor. Zu diesen Informationen zählen in der sich weiter beschleunigenden Digitalisierung von Wirtschaft und Gesellschaft immer häufiger auch personenbezogene Daten, d.h. Daten, die Rückschlüsse auf eine bestimmte oder jedenfalls bestimmbare Person ermöglichen.

Der Austausch persönlicher Daten, die teilweise höchst private Informationen betreffen, macht also an nationalen Grenzen nicht halt. Das erleben wir auch jeden Tag im Privat- und im Arbeitsleben. Datentransfers in andere Länder gehören mittlerweile zu unserem Alltag, bemerkbar oder nicht. Sei es als Mitglied in den sogenannten Sozialen Netzwerken oder bei der Nutzung von E-Mail-Diensten, Cloud-Services, Office-Anwendungen, Sensoren und Smart-Home-Geräten. Unsere Daten werden heute nicht mehr lokal, sondern global erhoben, gespeichert, verarbeitet und genutzt.

Für diese stetig wachsenden und zunehmend international verflochtenen Datenströme zwischen privaten Wirtschaftsteilnehmern interessieren sich auch staatliche Stellen, insbesondere die Sicherheitsbehörden.

Deren potentielle Erkenntnismöglichkeiten nehmen sozusagen im Gleichschritt mit der fortschreitenden Digitalisierung von Wirtschaft und Gesellschaft und der damit einhergehenden, ständig wachsenden Menge zur Verfügung stehender personenbezogener Daten zu.

Strafverfolgungs- und Sicherheitsbehörden erheben nicht mehr nur Daten direkt bei den betroffenen Personen. Seit vielen Jahren greifen diese Behörden auch auf Daten zu, die – zunächst einmal – durch private Stellen, z.B. von Telekommunikationsdiensteanbietern oder im Rahmen von Cloud-Computing-Dienstleistungen, verarbeitet werden. Ich erinnere hier nur an die sogenannten Passenger Name Records, also Fluggastdaten, die die internationalen Fluggesellschaften an Sicherheitsbehörden übermitteln müssen, oder an die für Corona-Dokumentations-Zwecke gesammelten Daten.

Dass die durch die Privatwirtschaft verarbeiteten Daten Begehrlichkeiten wecken, haben medienwirksam spätestens die Enthüllungen durch Edward Snowden und die dadurch bekannt gewordene Sammelwut der US-amerikanischen Sicherheitsbehörden gezeigt. Immer mehr Details werden auch vom chinesischen Überwachungsregime bekannt. Aber auch deutsche und europäische Sicherheitsbehörden haben für die Erledigung ihrer Aufgaben umfangreiche und tiefgreifende Zugriffsmöglichkeiten.

Um nicht missverstanden zu werden: Selbstverständlich gibt es Interessen, die es absolut rechtfertigen, dass staatliche Stellen im Rahmen ihrer Arbeit auch Kenntnis von personenbezogenen Daten erhalten, die von privaten Unternehmen und möglicherweise auch in anderen Ländern verarbeitet werden. Hierbei denke ich etwa an die Bekämpfung des internationalen Terrorismus und von organisierter Kriminalität wie Menschenhandel, Geldwäsche und Waffenhandel.

Die Frage ist dann allerdings, unter welchen Voraussetzungen dies erfolgt, welche Schranken gegen ein uferloses Datenzugriffsregime bestehen, welche Verfahren – Stichwort Rechtsstaatlichkeit – hierfür vorgesehen sind und wie die Rechte der Betroffenen ausgestaltet sind.

Mit genau diesen Fragen müssen sich europäische und das heißt auch deutsche Unternehmen beschäftigen, die Geschäftsbeziehungen in Staaten außerhalb der EU bzw. mit Unternehmen aus diesen Staaten unterhalten und in diesem Zuge auch personenbezogene Daten in diese Länder oder deren Rechtsraum übermitteln – im Datenschutzsprach-gebrauch sogenannte Drittstaaten oder Drittländer. Denn auch der Datenschutz endet nicht an nationalen Grenzen – und darf dort auch nicht enden.

Die staatlichen Eingriffsbefugnisse im Drittstaat, also in dem Zielland, in das oder in dessen rechtliche Reichweite die Daten übermittelt werden sollen, spielen für die Rechtmäßigkeit des Datentransfers eine wesentliche Rolle.

Um es auf den Punkt zu bringen: Die Frage, inwieweit und unter welchen Bedingungen ausländische Polizei- und Sicherheitsbehörden auf Daten zugreifen dürfen, ist nach der europäischen Datenschutzgrund-verordnung mitentscheidend dafür, ob die Übermittlung personen-bezogener Daten durch private Stellen in das jeweils betroffene Drittland überhaupt erlaubt ist. Staatliche Zugriffsbefugnisse, die nach europäischem Datenschutz- und Rechtsverständnis unverhältnismäßig sind, führen dementsprechend zu Beschränkungen und Restriktionen für die grenzüberschreitende Übermittlung personenbezogener Daten zwischen Unternehmen.

Es besteht also ein datenschutzrechtlicher Zusammenhang zwischen staatlichen Zugriffsbefugnissen auf der einen und dem internationalen Datenaustausch zwischen privaten Stellen auf der anderen Seite. Die privatwirtschaftliche Datenverarbeitung und die Datenverarbeitung durch staatliche Stellen sind hier eng miteinander verknüpft. Ob ein Daten-transfer zwischen einem Unternehmen in der EU und einem Unter-nehmen außerhalb der EU bzw. außerhalb der exklusiven Gültigkeit von EU-Recht zulässig ist, hängt davon ab, welche Regeln am Zielort für staatliche Zugriffe auf die zu übermittelnden Daten gelten.

Das europäische Unternehmen muss darauf vertrauen können, dass die personenbezogenen Daten nach der Übermittlung nach rechtstaatlichen Prinzipien verarbeitet werden. Wenn das nicht der Fall ist, bestehen Übermittlungsbeschränkungen für die personenbezogenen Daten. Dies wiederum kann gravierende Auswirkungen auf die wirtschaftlichen Aktivitäten europäischer Unternehmen im globalen Kontext haben und eine Hürde für unternehmerische Entscheidungen darstellen.

Auch das höchste europäische Gericht, der Europäische Gerichtshof, stellt bei der Frage, ob Daten in einen Drittstaat übermittelt werden dürfen, maßgeblich auf den dort bestehenden Schutz der Daten vor Zugriffen durch Sicherheitsbehörden ab. Vor diesem Hintergrund fällt es schwer zu begründen, dass eine Übermittlung personenbezogener Daten in ein Land datenschutzrechtlich zulässig sein soll, in dem rechtsstaatliche Grundsätze für das Handeln von Polizei- und Sicherheitsbehörden, wie wir sie in Deutschland und Europa kennen und praktizieren, nicht vorhanden sind.

Je weiter Wertevorstellungen und Grundprinzipien für staatliches Handeln auseinander liegen, desto schwieriger ist ein freier Datenfluss zwischen den Staaten bzw. den Rechtsräumen datenschutzrechtlich zu rechtfertigen.

Wo nicht nur ein unterschiedliches Datenschutzverständnis herrscht, sondern erhebliche datenschutzrechtliche und rechtstaatliche Bedenken bestehen, sind Datenübermittlungen äußerst problematisch und können – wenn überhaupt – in der Regel nur mit Hilfe von weiteren technischen Maßnahme zum Schutz der Daten durchgeführt werden. Ein solcher Fall kann meines Erachtens insbesondere dann angenommen werden, wenn das Maß an Überwachung übermäßig is, oder wenn es an ausreichenden Betroffenenrechten fehlt bzw. diese nicht effektiv geltend gemacht und unabhängig überprüft werden können. Die Frage ist nun, wie wir auf Dauer mit dieser Problematik umgehen und welche datenschutzrechtlich unabdingbaren Vorgaben wir für den Datentransfer in solche Länder fordern müssen.

II. Übermittlung personenbezogener Daten in sog. Drittstaaten

Mit der Datenschutzgrundverordnung haben wir in der gesamten Europäischen Union ein gleichmäßiges und hohes Datenschutzniveau etabliert, mit dem wahrlich nicht alle Länder der Erde mithalten können. Das Datenschutzverständnis in Ländern außerhalb der EU unterscheidet sich von dem in der Europäischen Union teilweise erheblich. Eine Ursache ist sicher, dass in der EU der Datenschutz von den Grundrechten abgeleitet wird, also mit anderen Grundrechten zusammen in der obersten rechtlichen Liga spielt.

Für die Übertragung personenbezogener Daten in Drittländer gelten daher besondere Anforderungen. Das europäische Datenschutzrecht erlaubt Datenübermittlungen in Drittstaaten, also in Länder oder Rechtsräume außerhalb der EU, nur unter bestimmten Voraussetzungen. Der wesentliche datenschutzrechtliche Grundsatz dabei ist, dass der Schutz der personenbezogenen Daten auch nach deren Übermittlung weiter gewährleistet sein muss.

Mit anderen Worten: Die Datenschutzstandards der EU sollen durch die Datenübermittlung nicht unterschritten werden. Die personenbezogenen Daten sollen auch nach der Übermittlung angemessen geschützt sein. Im Ergebnis bedeutet das, dass in dem Land, in das die Daten exportiert werden sollen, ein in der Sache gleichwertiges Datenschutzniveau sichergestellt sein muss.

Ob das der Fall ist, hängt maßgeblich von den im Drittstaat geregelten Eingriffsbefugnissen für die Polizei- und Sicherheitsbehörden ab. Die datenschutzrechtliche Unbedenklichkeit, d.h. ob ein im Wesentlichen vergleichbares Datenschutzniveau in einem Drittstaat angenommen werden kann, entscheidet sich nämlich nicht nur an den Datenschutzregelungen, die unmittelbar für den Datenempfänger, d.h. den Vertragspartner im Drittstaat, gelten.

Vielmehr muss der dort herrschende Rechtsrahmen daraufhin untersucht und bewertet werden, unter welchen Bedingungen staatliche Zugriffe auf personenbezogene Daten, die aus der EU übermittelt werden, erlaubt sind.

Hierfür sind die in dem Land gegebenen Rechtsschutzmöglichkeiten der betroffenen Personen von entscheidender Bedeutung. Der Government Access, also der Zugriff staatlicher Stellen auf personenbezogene Daten, stellt damit das zentrale Problem dar, das bei der Drittstaatenübermittlung personenbezogener Daten zu bedenken und zu bewerten ist.

Bei dieser Bewertung ist entscheidend, dass das insoweit betroffene Recht auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht nicht unkompliziert, aber sehr treffend formuliert hat, in der EU und in Deutschland wie erwähnt Verfassungsrang hat. Danach ist Datenschutz ein in der deutschen und auch in der europäischen Verfassung verankertes Grundrecht. Dieser Grundrechtsschutz muss auch im internationalen Datenverkehr gewährleistet werden.

So hat der Europäische Gerichtshof, und ich denke hier insbesondere an die beiden sogenannten Schrems-Verfahren, in seinen Entscheidungen immer wieder deutlich gemacht, dass der Schutz personenbezogener Daten und die Achtung der Privatsphäre als europäische Grundrechte auch im internationalen Datenverkehr beachtet werden müssen.

Wie bereits angesprochen, erschweren diese Vorgaben allerdings den ungehinderten internationalen Datenaustausch und sind von erheblicher wirtschaftlicher Tragweite. Europa ist Teil der globalen Wirtschaft und der internationalen Digitalisierung. Vor diesem Hintergrund stellt sich aktuell die Frage, wie mit diesem Dilemma umgehen?

Diese Fragestellung stand in diesem Jahr auch im Mittelpunkt verschiedener internationaler Initiativen. Die Global Privacy Assembly, das ist ein weltweiter Zusammenschluss regionaler, nationaler und internationaler Datenschutzbehörden, hat im Oktober gemeinsame Prinzipien für „Government Access“, also den staatlichen Zugriff auf personenbezogene Daten, beschlossen.

Auch auf Ebene der OECD – der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung – wird an solchen gemeinsamen Datenschutzgrundsätzen gearbeitet.

Daran anknüpfend haben erst kürzlich auch die Datenschutzaufsichts-behörden der G7-Staaten das Thema „Government Access“ diskutiert.

Die Tatsache, dass dieses Thema auch in globalen Datenschutzforen und der internationalen Datenschutzpolitik angekommen ist, also nicht mehr nur von Datenschutzexperten in kleinen Zirkeln diskutiert wird, zeigt einmal mehr die Bedeutung des freien Datenverkehrs für die weltweite digitale Wirtschaft und damit für den Wohlstand der einzelnen Volkswirtschaften.

Die Entwicklungen der letzten Jahre haben in der Tat deutlich gemacht, dass das Fehlen ausreichender internationaler Datenschutzgarantien nicht nur ein Risiko für den Schutz personenbezogener Daten darstellt, sondern auch erhebliche wirtschaftliche Auswirkungen hat. Da der Datenschutzstandard gerade in großen Ländern, in denen sich europäische Unternehmen stark engagieren bzw. in die europäische Unternehmen viele Geschäftsbeziehungen pflegen – wie etwa China oder die USA – nicht dem europäischen Datenschutzniveau entspricht, besteht für die europäische Wirtschaft die Gefahr, dass der Datenverkehr mit ganzen Märkten erheblich eingeschränkt werden könnte.

III. Datenschutz vs. Innovation und wirtschaftlicher Erfolg?

In der öffentlichen Debatte werden Digitalisierung und Datenschutz oft als unvereinbare Gegensätze dargestellt. In diesem Zusammenhang höre ich – mal mehr, mal weniger vorwurfsvoll formuliert – immer wieder die folgenden Fragen:

Ist es angesichts der neuen Möglichkeiten, die die Digitalisierung bietet, wirklich sinnvoll, an den strengen europäischen datenschutzrechtlichen Vorgaben festzuhalten?

Bremst der Datenschutz nicht den technologischen Fortschritt und die wirtschaftliche Entwicklung aus?

Werden Deutschland bzw. die Europäische Union aufgrund ihrer strikten Datenschutzregelungen im Rahmen einer global agierenden Wirtschaft abgehängt, so dass Wachstum und Wohlstand Schaden nehmen?

Die Sichtweise, die hinter diesen Fragen steht, halte ich für gefährlich und falsch. Dem Datenschutz kommt bei der Digitalisierung eine besondere Aufgabe zu: Datenschutz kann und muss die technische Entwicklung konstruktiv begleiten, als Garant für die Wahrung der Grundrechte. Er stärkt bestimmte Technologien, hemmt aber Geschäftsmodelle, die mit europäischen Werten nicht vereinbar sind. Damit unterscheidet er sich in seiner Wirkung nicht vom Schutz von Kindern (Kinderarbeit), Umweltschutz, Vertragsrecht und Strafrecht.

Der Datenschutz muss bei der Entwicklung neuer Projekte und Programme von Anfang an mitgedacht und mitentwickelt werden, dann ist er nicht etwa Kostentreiber, sondern sogar Innovationsmotor.

Ein starker Datenschutz ist unabdingbar für eine ethische und gerechte Ausgestaltung unserer digitalen Zukunft. Es ist ein Irrglaube, dass es der Digitalisierung helfe, möglichst wenig zu regulieren und bestehende gesetzliche Vorgaben weitestgehend abzuschaffen.

Eine wohlverstandene Regulierung dient vielmehr dazu, die beteiligten Interessen in einen angemessenen Ausgleich zueinander zu setzen und dabei die Werte unserer Rechtsordnung zu gewährleisten und die Grundrechte der Betroffen zu schützen.

Wie ich schon sagte, ist Datenschutz in Deutschland und Europa von den Grundrechten abgeleitet und nicht beliebig. Das Grundrecht auf Datenschutz steht nicht zur Disposition.

Datenschutz ist aber auch kein Selbstzweck: Wie alle Grundrechte steht er in einer Wechselwirkung mit den Werten von Demokratie und Rechtsstaatlichkeit. Einerseits wird er erst durch demokratische Strukturen wirklich ermöglicht. Andererseits trägt er in vielerlei Hinsicht dazu bei, unsere freiheitlich demokratische Grundordnung zu erhalten.

Datenschutz ermöglicht es Bürgerinnen und Bürgern möglichst frei darüber zu entscheiden, was und wieviel sie anderen über sich preisgeben wollen, wenn sie ihre vielfältigen Freiheitsrechte ausüben, als Einzelperson und in Gruppen, von der öffentlichen Meinungsäußerung bis zur privaten Vorliebe und dem Schutz vor Diskriminierung. Der Datenschutz schützt die Persönlichkeitsrechte des Einzelnen, ohne die eine verantwortungsbewusste und gesellschaftlich sinnvolle und nachhaltige technologische Weiterentwicklung kaum möglich ist.

Der Datenschutz darf nicht als Innovationshindernis diskreditiert werden, der den technologischen Fortschritt ausbremst oder Investoren abschreckt.

Datenschutz ist kein Hemmschuh für Innovationen, er fördert diese sogar, wenn die Nutzer Vertrauen in die Sicherheit und die Fairness neuer Technologien haben. Hierzu stelle ich noch einmal ausdrücklich fest: Handlungs- und Geschäftsmodelle, die den Datenschutz missachten, sind weder nachhaltig noch innovativ. Das gilt für den Zugriff staatlicher Stellen, aber auch die Datensammlungen und –auswertungen privater Akteure.

In diesem Zusammenhang kommt immer wieder der Hinweis auf die weit entwickelten Digitalökonomien in China oder den USA, deren technologischer Vorsprung als quasi „uneinholbar“ beschrieben und als Druckmittel für ein „Absenken“ der europäischen Datenschutzstandards genutzt wird. Diese Sichtweise ist gefährlich und birgt die Gefahr einer Abwärtsspirale.

Die Antwort auf laxere Datenschutzregeln in anderen Ländern kann nicht die Forderung sein, das eigene Datenschutzniveau herunterzusetzen. Wenn man diesen Gedanken weiterspinnt, zeigt sich, dass dadurch ein „race to the bottom“ entstehen würde, das heißt ein Unterbietungs-wettlauf, der zu einem stetigen Abbau datenschutzrechtlicher Standards führt.

Und das ist auch richtig und wichtig.

Ein Beispiel für ein entsprechendes „Negativ-Benchmark“ in diesem Kontext wäre das Angebot der Chinesischen Regierung, ausländischen Forschungsunternehmen, die sich in einer bestimmten Region ansiedeln, den Zugriff auf hunderttausende realer Gesundheitsdaten der chinesischen Bevölkerung zu gewähren.

Aber wie sieht die Alternative hierzu aus? Den zum Teil vertretenen Ansatz von einer buchstäblichen digitalen europäischen Autarkie halte ich nicht für erfolgsversprechend. Ein digital autarker Staat bzw. Wirtschaftsraum würde sich ausschließlich mit eigenen Angeboten aus eigenen Ressourcen versorgen – auch wenn die Produkte weniger leistungsfähig sind als entsprechende Angebote Dritter außerhalb des eigenen Territoriums.

Eine digitale Autarkie würde weit über das berechtigte Anliegen einer digitalen Souveränität, also einer Unabhängigkeit, in Richtung eines Abkapselns und einer Selbstisolierung hinausgehen. Nicht nur europäische Unternehmen, die längst weltweit agieren, wären dann vor eine kaum zu lösende Aufgabe gestellt. Auch wäre der europäische Raum mit seinen knapp 450 Millionen Einwohnerinnen und Einwohner immer noch zu klein, um andere Staaten auf der Welt davon zu überzeugen, sich digital an uns statt an die USA oder an China anzulehnen.

Autarkie ist in einer global vernetzten digitalen Welt weder zu erreichen noch anzustreben.

Souveränität schon und vor allem technologische und rechtliche Alternativen zur chinesischen Staatswirtschaft mit totalitärem Überwachungsapparat und dem US-amerikanischen laissez-faire mit einem Überwachungsapparat mit doppeltem Maßstab für eigene und fremde Bürger:innen.

IV. Idee und Ziel eines gemeinsamen Datenraums des Westens

Das alles zeigt, dass Datenschutzstandards nicht nur auf einzelne Länder oder kleinere Staatengemeinschaften beschränkt bleiben sollten, sondern ein globales Anliegen sein müssen. Mindestens für die Grundregeln staatlichen Zugriffs, besser noch auch für die allgemeinen Datenschutzregelungen.

Es ist wichtig, dass wir uns innerhalb Europas und darüber hinaus dafür einsetzen, dass es ein breites gemeinsames Verständnis für den Schutz der Grundrechte und damit auch für den Datenschutz gibt. Das erfordert eine internationale Zusammenarbeit und kooperative Regulierungs-ansätze.

Deutschland und Europa sollten Antreiber für solch ein gemeinsames Verständnis zwischen den liberal und demokratisch regierten Staaten dieser Erde werden, um einen gemeinsamen Datenraum auf der Grundlage geteilter Werte zu schaffen, der den freien Datenverkehr auf einem hohen Schutzniveau der Grundrechte vor staatlichem Zugriff ermöglicht und in dem dann auch noch unterschiedliche Datenschutz-regelungen für den privaten Sektor wirken können.

Digitale Innovationen und wirtschaftlicher Wohlstand mit den westlichen Werten einer liberalen Demokratie zu kombinieren wäre dann das attraktive Gegenmodell zu den Entwicklungspfaden, die autoritäre Regime vorleben. Das wäre eine Win-Win-Situation für die Menschen und die Unternehmen. Ein gemeinsamer Datenraum würde digitale Innovationen, gemeinsame Forschungsprojekte mit intensiver Datenauswertung und sinkende Kosten für digitale Angebote ermöglichen.

Gleichzeitig würden wohl zunehmend auch allgemeingültige hohe Datenschutzstandards für private Geschäftsmodelle und Forschungsvorhaben gesetzt, weil global agierende Unternehmen und Forschungsvorhaben von vereinheitlichten Regelungen profitieren würden. Der gemeinsame Datenraum würde einen Markt schaffen, an dem die Wirtschaft mit datenschutzfreundlichen Lösungen punkten kann und wo hohe Datenschutzstandards zentrale Qualitätsmerkmale sind. Diese Lösungen hätten übrigens selbst außerhalb dieses Datenraums einen Markt und positive Auswirkungen.

Dies dürfte von den Verbraucherinnen und Verbrauchern begrüßt werden, die von einem derartigen Datenschutzniveau ja nicht nur als Konsumenten von Produkten und Dienstleistungen profitieren, sondern auch im Hinblick auf mögliche Zugriffe staatlicher Stellen in ihrer Privatsphäre betroffen sind.

In einem gemeinsamen Datenraum könnten Bereiche von gegenseitigem Interesse oder Chancen erkannt werden, um flexibel auf laufende Entwicklungen zu reagieren und gleichzeitig für Kohärenz und Rechtssicherheit zu sorgen. Trotzdem könnten noch unterschiedliche Regelungen für den Datenschutz im privaten Sektor und auch für den öffentlichen Sektor, wo er sich vor allem an die eigenen Bürger:innen richtet, gelten. Die DSGVO würde nicht obsolet, sondern sogar gestärkt. Sie würde weiter einen Standard setzen, an dem sich andere orientieren, wie zuletzt Japan, Südkorea und Kalifornien.

Noch einmal zurück zur falschen Überschrift meines Vortrags „Trau, schau wem – der Westen braucht einen gemeinsamen Datenraum“. Was meine ich damit? Wer ist „der Westen“ – und wer ist es nicht?

Mit diesem – ich gebe es zu – etwas plakativen Begriff ist keine geographische Beschränkung eines gemeinsamen Datenraums verbunden. Ganz im Gegenteil, der Idee eines gemeinsamen Datenraums können und sollen sich Länder aus allen Regionen der Welt anschließen. In Lateinamerika, in Asien und Afrika gibt es quasi natürliche Kandidaten für diesen gemeinsamen Datenraum. Es geht um mehr als USA, Kanada, Europa und Australien. Südkorea, Mexiko, Brasilien, Südafrika, Indien und viele kleinere Länder wären wichtige Säulen dieses gemeinsamen Datenraums.

Mit dem Vorhaben eines gemeinsamen Datenraums soll eben gerade keine exklusive Gruppe von Volkswirtschaften geschaffen werden, die andere ausschließt. Ich stelle mir vielmehr vor, dass der gemeinsame Datenraum ein Angebot darstellen sollte, mitzumachen.

Wichtig ist, dass die Vorzüge eines gemeinsamen Datenraums für andere Staaten sichtbar werden. Sie sollen Teil eines Wirtschaftsraums mit einem freien und damit wirtschaftlich attraktiven Datenverkehr unter Beachtung datenschutzrechtlicher Prinzipien werden wollen.

In dem Begriff „der Westen“ kommt für mich daher vielmehr eine gemeinsame Werteordnung zum Ausdruck, wie sie in vielen westlichen Ländern gelebt wird. Dahinter verbirgt sich ein gemeinsamer Wertekodex, der das staatliche Handeln in diesen Ländern prägt und leitet. Dazu zählen Demokratie, Rechtsstaatlichkeit, Gewaltenteilung und die Unabhängigkeit der Justiz. Letzteres möchte ich angesichts jüngster besorgniserregender Entwicklungen auch innerhalb der EU ganz besonders betonen. Es geht also um liberale demokratische Gesellschaften.

In der europäischen Digitalpolitik wird bereits seit Längerem das Konzept der „digitalen Souveränität“ diskutiert. Anfang des Jahres hat die Europäische Kommission einen digitalen Kompass vorgestellt, wie die Digitalziele der Europäischen Union bis 2030 konkret umgesetzt werden sollen.

Die Europäische Kommission ist entschlossen, das kommende Jahrzehnt zur digitalen Dekade Europas zu machen. Dreh- und Angelpunkt dieses digitalen Wandels ist der Ausbau der europäischen digitalen Souveränität.

Hinter diesem Begriff steckt die Idee einer digitalen Unabhängigkeit. Die Bürgerinnen und Bürger, die Unternehmen und die europäische Staatengemeinschaft sollen digital selbstbestimmt handeln können.

„Digitale Souveränität“ bezeichnet in diesem Sinne die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum. Digital souveräne Systeme können eigene strategische digitale Ziele ganzheitlich definieren und umsetzen. Sie sind in der Lage, selbstbestimmt und selbstbewusst zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner zu entscheiden, sie bewusst und verantwortungsvoll einzusetzen und sie im Bedarfsfall weiterzuentwickeln, ohne ausschließlich auf eigene Ressourcen zurückgreifen zu müssen.

Die Idee einer digitalen Souveränität grenzt sich also auf der einen Seite gegenüber autarken Systemen, die sich ausschließlich selbst versorgen, und auf der anderen Seite gegenüber einem Zustand der Fremdbestimmung ab, in dem die Abhängigkeit von Dritten so groß ist, dass kein eigenständiger Handlungsspielraum verbleibt.

Auch ich als Bundesdatenschutzbeauftragter setze mich für die Stärkung einer digitalen europäischen Souveränität ein.

Wie passt das aber zu der Forderung nach einem gemeinsamen Datenraum des Westens? Ich möchte ganz klar sagen: Diese Forderung ist keine Abkehr von dem Konzept einer digitalen europäischen Souveränität. Mir ist nur wichtig, über den eigenen Tellerrand hinaus-zuschauen.

Denn das Ziel der digitalen Souveränität birgt neben vielen Chancen auch ein Risiko: Sie sollte nicht zu Protektionismus à la „made in Europe first“ führen. Digitale Souveränität darf nicht verstanden werden als ein Abschied von globalisierten Produktions-, Innovations- und Wertschöpfungsprozessen. Sie darf nicht zu einer Abkehr von der gar nicht so naiven Idee führen, dass wir die Digitalisierung für eine Verbreitung von Partizipation, Liberalität, Nachhaltigkeit und Wohlstand nutzen können. Ich bin nicht bereit, diese Idee aufzugeben.

Es ist Realität, dass Machtprojektion und Einflussnahme auf internationaler Ebene in zunehmendem Maße mithilfe digitaler Technologien ausgeübt werden. Die EU muss sich daher auch über ihre Grenzen hinweg in Gespräche und Verhandlungen über die Gestaltung des digitalen Raums einbringen. Wir dürfen uns nicht zurückziehen auf einen rein europäischen Standpunkt, es kann keinen digitalen Isolationismus geben.

In diesem Sinne ist ein gemeinsamer Datenraum des Westens eine logische Fortsetzung und gewissermaßen Erweiterung des Anliegens einer europäischen digitalen Souveränität.

V. Eine Vereinbarung für einen gemeinsamen Datenraum?

Auf welcher Grundlage kann der gemeinsame Datenraum entstehen? Was wären die Grundpfeiler des gemeinsamen Datenraums?

Ein gemeinsamer Datenraum heißt, wie schon erwähnt, sicher nicht, dass sich die daran beteiligten Staaten auf ein gemeinsames unmittelbar geltendes umfassendes Datenschutzrecht einigen. Der Versuch, ein solches Ziel anzustreben, wäre unrealistisch und von vornherein zum Scheitern verurteilt.

Ein gemeinsamer Datenraum müsste aber auf gemeinsamen daten-schutzrechtlichen Grundprinzipien aufbauen, die in den Rechts-ordnungen der verschiedenen Staaten umgesetzt sind. Dabei kann die Umsetzung der gemeinsamen Datenschutzgrundsätze von Land zu Land verschieden ausfallen. Das Ziel muss sein, einen übergreifenden daten-schutzrechtlichen Mindeststandard im gemeinsamen Datenraum zu etablieren und zu wahren.

Hierfür können dann im Einzelnen und zum Beispiel abhängig von bestehenden Rechtssystemen und -traditionen durchaus unter-schiedliche Wege beschritten werden; die gemeinsamen Prinzipien müssen in den einzelnen Ländern also nicht in identischer Art und Weise umgesetzt werden.

Entscheidend ist aber, dass sie im Ergebnis dazu führen, ein in der Sache gleichwertiges Schutzniveau für die Bürgerinnen und Bürger im gemeinsamen Datenraum zu schaffen, mindestens gegenüber staatlichen Zugriffen auf personenbezogene Daten.

Einen ähnlichen Ansatz sieht übrigens schon die europäische Datenschutzgrundverordnung für Datenübermittlungen in außereuropäische Länder vor. Für die aus der EU übermittelten Daten muss im Drittland ein Schutzniveau gewährleistet sein, das mit dem unionsrechtlichen Datenschutzniveau im Wesentlichen vergleichbar ist.

Diese Anforderung des europäischen Datenschutzrechts gilt fort. Europäische Datenschutzstandards dürfen – auch im Rahmen des von mir heute vorgestellten gemeinsamen Datenraums – nicht unterschritten werden.

Nun fragen Sie sich hoffentlich interessiert, welche Grundprinzipien denn nun ganz konkret geregelt werden müssten. Hierfür kann ich auf die Arbeiten der schon erwähnten Initiativen der Global Privacy Assembly und der OECD und der G7-Gruppe Bezug nehmen, an denen ich beteiligt war. Diese Initiativen zeigen im Übrigen, dass die Frage nach gemeinsamen Datenschutzstandards kein lediglich deutsches oder europäisches Thema ist, sondern mittlerweile global diskutiert wird.

Die Sicherstellung eines angemessenen datenschutzrechtlichen Schutzes von Menschen gegen unangemessene Zugriffe staatlicher Stellen auf ihre Daten, die aufgrund und im Rahmen der sich stetig weiterentwickelnden Digitalisierung weltweit erhoben und verarbeitet werden, ist ein Anliegen vieler.

Jetzt zu einigen konkreten Inhalten:

1. Gesetzliche Rechtsgrundlage

Jede Verarbeitung personenbezogener Daten durch staatliche Stellen stellt einen Eingriff in das Recht auf Datenschutz dar. In der deutschen und auch in der europäischen Rechtstradition spricht man vom Recht auf informationelle Selbstbestimmung. Geschützt ist das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. In Deutschland und Europa handelt es sich dabei um ein Grundrecht.

Ein Eingriff in das Recht auf Datenschutz darf nur zulässig sein, wenn er gesetzlich vorgesehen ist; er bedarf einer transparenten gesetzlichen Rechtsgrundlage. Die Grenzen zulässiger und unzulässiger Datenverarbeitung müssen vom Gesetzgeber bestimmt werden. Als ein Kernprinzip des gemeinsamen Datenraums muss daher geregelt werden, dass die Befugnisse staatlicher Stellen zur Verarbeitung personenbezogener Daten transparent durch den Gesetzgeber festgelegt werden.

2. Grundsatz der Verhältnismäßigkeit

Das allein reicht jedoch nicht aus. Die Forderung nach einer gesetzlichen Regelung von staatlichen Zugriffsbefugnissen greift für sich allein genommen zu kurz. Die Rechtsgrundlage selbst muss bestimmten Anforderungen genügen.

Insbesondere muss eine gesetzliche Regelung, die zu einer Einschränkung des Rechts auf Datenschutz führt, verhältnismäßig sein bzw. die staatlichen Befugnisse verhältnismäßig ausgestalten und regeln.

Der Grundsatz der Verhältnismäßigkeit leitet sich aus dem Rechtsstaatsprinzip ab und muss als „Übermaßverbot“ alle staatliche Gewalt binden. Der Grundsatz der Verhältnismäßigkeit ist nur gewahrt, wenn der Zugriff auf personenbezogene Daten und deren spezifische Verwendung für eine nachweislich notwendige Aufgabe der für diese Tätigkeit zuständigen Behörde erforderlich ist.

Das wiederum bedeutet, dass der Behörde keine anderen Möglichkeiten oder Maßnahmen zur Verfügung stehen dürfen, mit denen sie ihre Aufgabe auf eine weniger belastende, weniger eingriffsintensive Art und Weise erledigen können. Zum Beispiel wenn das Ziel der staatlichen Maßnahme auch ohne oder jedenfalls durch einen weniger umfangreichen Zugriff auf personenbezogene Daten erreicht werden kann.

Es reicht also nicht aus, wenn die Rechtsgrundlage lediglich auf die bloße Möglichkeit abstellt, den Zweck des staatlichen Handelns durch die Datenverarbeitung zu erreichen, ohne mögliche Alternativen in den Blick zu nehmen.

Anders ausgedrückt: Schon in der Rechtsgrundlage muss angelegt sein, dass die widerstreitenden Interessen, nämlich das staatliche Interesse an der Datenverarbeitung auf der einen und die Persönlichkeitsrechte der Betroffenen auf der anderen Seite, gegeneinander abgewogen und zu einem Ausgleich gebracht werden, der beide Interessen möglichst weitgehend berücksichtigt.

Die Bedeutung des Ziels, das mit der Einschränkung verfolgt wird, muss der Schwere des Eingriffs in das Recht auf Schutz personenbezogener Daten angemessen sein. Sprich, die Schwere des mit der Datenverarbeitung bewirkten Eingriffs in die Persönlichkeitsrechte der Betroffenen darf bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der den Datenzugriff rechtfertigenden Gründe stehen.

3. Betroffenenrechte

Den betroffenen Personen, auf deren Daten zugegriffen wird, müssen eigene Rechte gegenüber den Stellen eingeräumt werden, die ihre Daten verarbeiten. Es müssen ihnen Werkzeuge an die Hand gegeben werden, um sich über den Umgang mit ihren Daten zu informieren und die Datenverarbeitung kontrollieren zu können.

Klare und eindeutige Rechte der betroffenen Personen gehören zu den Grundlagen des Datenschutzes. Das Recht auf Auskunft, also zu erfahren, ob und welche Daten über mich verarbeitet werden oder das Recht auf Löschung von meinen persönlichen Informationen, wenn diese nicht mehr benötigt werden, sind die Basis der informationellen Selbstbestimmung. Sie dienen der Transparenz und einer fairen Datenverarbeitung und bewirken zudem eine Kontrolle der Datenverarbeitung durch die Betroffenen.

Anzuerkennen ist jedoch auch, dass im Rahmen der Datenverarbeitung durch Strafverfolgungs- und Sicherheitsbehörden gewisse Einschränkungen von Betroffenenrechten legitim und gerechtfertigt sein können. Wenn die Erteilung einer Auskunft zum Beispiel die öffentliche Sicherheit oder Dritte gefährden würde, kann es auch zulässig sein, das Auskunftsrecht zu beschränken. In derartigen Fällen sollte dann geprüft werden, ob das Betroffenenrecht gegebenenfalls zu einem späteren Zeitpunkt nachgeholt werden kann, zum Beispiel wenn von einer Auskunftserteilung keine Gefahr mehr ausgeht. Oder wenigstens unabhängige Aufsichten an die Stelle der individuellen Auskünfte treten.

4. Effektiver Rechtsschutz

Ein ganz zentraler und mit den Betroffenenrechten eng verbundener Aspekt sind die Rechtsschutzmöglichkeiten der betroffenen Personen. Diese müssen wirksame Rechtsbehelfe und Rechtsmittel gegen die Verarbeitung ihrer Daten einlegen und das staatliche Handeln gerichtlich überprüfen lassen können.

Effektiver Rechtsschutz hat eine herausgehobene Bedeutung. Dies gilt ganz besonders im Bereich der polizeilichen und nachrichtendienstlichen Datenverarbeitung, in dem Betroffenenrechte wie das Recht auf Auskunft oder andere Informationsrechte – wie oben angesprochen – eingeschränkt sein können.

Dann ist es unabdingbar, dass die Betroffenen eine gerichtliche Kontrolle der Datenverarbeitung anstrengen können. In solchen Fällen darf der Zugang zu Gerichten nicht beschränkt sein. In diesem Zusammenhang wäre es zum Beispiel problematisch, die Möglichkeit, ein Gericht anzurufen, davon abhängig zu machen, dass der Kläger seine individuelle Betroffenheit nachweist, also darlegt, dass ganz konkret seine Daten verarbeitet werden. Denn diese Nachweismöglichkeit besteht praktisch nicht, wenn Auskunfts- oder Informationsrechte beschränkt sind.

Da die Polizei- und Sicherheitsbehörden häufig heimlich und ohne Mitwirkung der Betroffenen auf persönliche Informationen zugreifen, können diese dann gar nicht wissen, ob ihre Daten verarbeitet werden.

Hier wird auch deutlich, wie wichtig gegebenenfalls nachträglich zu erfüllende Informationspflichten für die Wirksamkeit von Rechtsbehelfen sind. Denn betroffene Personen haben häufig kaum Anlass den Rechtsweg zu beschreiten, wenn sie nicht über die regelmäßig ohne ihr Wissen durchgeführten behördlichen Datenzugriffe in Kenntnis gesetzt werden.

5. Unabhängige Datenschutzaufsicht

Ein weiterer wesentlicher Datenschutzgrundsatz betrifft die Kontrolle durch eine unabhängige Datenschutzaufsicht. Die Betonung liegt hierbei auf unabhängig. Dies halte ich für zwingend erforderlich. Kontrollstellen sind vor jeder äußeren Einflussnahme zu bewahren. Nur so können sie die ihnen zugewiesenen Aufgaben effektiv erfüllen.

Die Notwendigkeit einer völligen Unabhängigkeit hat nicht zuletzt der EuGH in Bezug auf meine Behörde festgestellt, die bis 2016 im Bundesinnenministerium angesiedelt war und der Rechtsaufsicht durch die Bundesregierung unterstand. Die damals immerhin bestehende funktionelle Unabhängigkeit hat das Gericht als nicht ausreichend erachtet. Heute untersteht das Amt des Bundesdatenschutzbeauftragten daher ausschließlich der parlamentarischen und gerichtlichen Kontrolle.

Zentrales Element einer wirksamen Aufsicht und Kontrolle ist zudem, dass Aufsichtsbehörden verbindliche und durchsetzbare Maßnahmen gegenüber den öffentlichen Stellen, die ihrer Aufsicht unterliegen, treffen können. Aufsichtsbehörden müssen über ausreichende Durchsetzungsbefugnisse verfügen, die es ihnen ermöglichen, die Einhaltung der Datenschutzrechte wirksam sicherzustellen und verbindliche Maßnahmen zu treffen.

Um eine effektive Aufsicht sicherstellen zu können, muss diese zudem über ausreichende Ressourcen und Mittel verfügen. Dazu zählen

personelle Ressourcen aber auch eine angemessene Ausstattung in finanzieller und in technischer Hinsicht.

VI. Ausblick und Rolle des BfDI

Um den von mir vorgestellten Datenraum Wirklichkeit werden zu lassen, muss die internationale Staatengemeinschaft bzw. eine große Gruppe darin nun die erforderlichen Schritte einleiten. Es ist notwendig, einheitliche und hohe Datenschutzstandards zu vereinbaren, die insbesondere den Government Access regeln. Dabei kann an die Arbeiten und Ergebnisse der laufenden internationalen Bemühungen, gemeinsame Datenschutzgrundsätze zu vereinbaren, angeknüpft werden.

Dies ist auch von den G7-Staaten erkannt und diskutiert worden, als im September dieses Jahres erstmalig ein Treffen der Datenschutz-aufsichtsbehörden der G7-Länder stattgefunden hat. Dabei ging es maßgeblich darum, Möglichkeiten für eine engere Zusammenarbeit auszuloten, um den Datenschutz in diesem digitalen Zeitalter zu sichern und auszubauen.

Die Datenschutzaufsichtsbehörden müssen immer besser in der Lage sein, die Fortschritte bei der Datennutzung zu antizipieren, zu interpretieren und zu beeinflussen. Dafür ist eine stärkere Vernetzung auch unter den Behörden notwendig.

Wir haben vereinbart, unsere nationalen Bemühungen zur Förderung ehrgeiziger Grundsätze für eine Regulierung des staatlichen Zugangs zu personenbezogenen Daten stärker zu koordinieren und auch mit unseren jeweiligen Regierungen zusammenzuarbeiten, um gemeinsame Prinzipien für den staatlichen Zugriff auf personenbezogener Daten, die durch private Stellen verarbeitet werden, aufzustellen.

Ein wichtiger Grundstein für das Vorhaben eines gemeinsamen Datenraums ist damit gelegt worden. Erste Überzeugungsarbeiten wurden geleistet.

Ich bin bereit, hier weiter die Initiative zu ergreifen und auf meine europäischen und internationalen Kolleginnen und Kollegen zuzugehen und die Idee eines gemeinsamen Datenraumes – über die Grenzen der EU hinaus – sowie einen engeren Austausch mit den relevanten Stakeholdern voranzutreiben. Eine gute Gelegenheit dafür wird sich im kommenden Jahr bieten, wenn Deutschland, d.h. meine Behörde, Gastgeber für den Runden Tisch der G7-Datenschutzaufsichtsbehörden sein wird. Ich werde dann darauf achten, dass nicht nur staatliche Stellen, WEF und OECD an der Diskussion beteiligt sind, sondern ich werde die Zivilgesellschaft, die Nicht-Regierungsorganisationen in diesen Prozess intensiv einbinden.

Eins ist aber klar: Selbst wenn der von mir vorgestellte gemeinsame Datenraum einmal Wirklichkeit werden sollte, wird er Grenzen haben. Es wird weiter Staaten geben, die die Prinzipien und Grundsätze, und das heißt auch die dahinter stehenden gemeinsamen Werte dieses Raumes, nicht teilen und nicht unterstützen. Das wird die Frage mit sich bringen, wie der gemeinsame Datenraum sich diesen Ländern gegenüber aufstellt. Welche Anforderungen sollen für Datenübermittlungen über die Grenzen des gemeinsamen Datenraums hinaus gelten? Dies wird insbesondere dann virulent werden, wenn diese Staaten wirtschaftlich mächtig sind. Hier wird sich werteorientierte Politik dann bewähren müssen.

Sehr geehrte Damen und Herren, ich freue mich nun auf die Diskussion und danke Ihnen für Ihre Aufmerksamkeit.