EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 4/2015

Der Weg zu einem neuen digitalen Ethos

Daten, Würde und Technologie

11. September 2015

Der Europäische Datenschutzbeauftragte (EDSB) ist ein unabhängiges Organ der EU und hat gemäß Artikel 41 Absatz 2 der Verordnung 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten ... sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden" und ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und spezifisch mit einem konstruktiveren und proaktiveren Vorgehen beauftragt. In der im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

Diese Stellungnahme schließt sich an die vorherige Stellungnahme des EDSB zu der Allgemeinen Datenschutzverordnung an, die darauf abzielte, die Hauptorgane der EU bei der Erzielung eines geeigneten Konsens über ein praktikables, zukunftsorientiertes Regelwerk, das die Rechte und Freiheiten natürlicher Personen untermauert, zu unterstützen. Wie schon in der Stellungnahme zu Mobile-Health-Diensten im Frühjahr 2015 geht es auch in dieser Stellungnahme um die Herausforderung, den Datenschutz an die digitale Welt anzupassen, - dem dritten Ziel der EDSB-Strategie - „um bestehende Datenschutzprinzipien für die globale digitale Arena anzupassen" auch im Lichte der Pläne der EU für einen digitalen Binnenmarkt. Sie stimmt mit dem Ansatz der Artikel-29-Datenschutzgruppe in Bezug auf Datenschutzaspekte der Verwendung neuer Technologien wie dem „Internet der Dinge", zu dem der EDSB als Vollmitglied der Gruppe beitrug, überein.

Dignity	**Würde**
Future oriented rules and enforcement	**Zukunftsorientierte Regeln und Durchsetzung**
Empowered individuals	**Menschen mit gestärkter Handlungskompetenz**
Accountable controllers	**Rechenschaftspflichtige Verantwortliche**
Innovative privay engineering	**Innovatives Datenschutz-Engineering**
Ethics	**Ethos**

„Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen."

Artikel 1, EU-Charta der Grundrechte

Die Grundrechte auf den Schutz der Privatsphäre und auf den Schutz personenbezogener Daten sind für den Schutz der Menschenwürde wichtiger denn je geworden. Sie sind in den EU-Verträgen und in der EU-Charta der Grundrechte verankert. Sie versetzen Menschen in die Lage, ihre eigene Persönlichkeit zu entwickeln, unabhängig zu leben, Neues zu schaffen und andere Rechte und Freiheiten auszuüben. Die in der EU-Charta definierten Datenschutzgrundsätze - Notwendigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Datenminimierung, Beschränkung auf den jeweiligen Zweck, Einwilligung und Transparenz - gelten für die Datenverarbeitung in ihrer Gesamtheit, und zwar sowohl für die Erhebung als auch die Nutzung.

Zwar sollten Werte und Rechte nicht durch Technologie bestimmt werden, ihre Beziehung zueinander sollte aber auch nicht auf eine unechte Dichotomie reduziert werden. Die digitale Revolution verspricht Vorteile für Gesundheit, Umwelt, internationale Entwicklung und wirtschaftliche Effizienz. Gemäß den Plänen der EU für einen digitalen Binnenmarkt gelten Cloud-Computing, das „Internet der Dinge", Big Data und andere Technologien als ausschlaggebend für Wettbewerbsfähigkeit und Wachstum. Geschäftsmodelle profitieren von neuen Möglichkeiten zur Erhebung von Daten im großen Maßstab, zur sofortigen Datenübermittlung sowie zur Kombinierung und Wiederverwendung von personenbezogenen Informationen für unvorhergesehene Zwecke auf der Grundlage von langen und undurchsichtigen Datenschutzrichtlinien. Die Datenschutzgrundsätze unterliegen dadurch neuen Belastungen, weshalb ihre Anwendung innovativ überdacht werden muss.

In der heutigen digitalen Umgebung reicht das Befolgen von Gesetzen nicht aus; die ethische Dimension der Datenverarbeitung muss berücksichtigt werden. Innerhalb des Rechtsrahmens der EU besteht bereits Raum für flexible, von Fall zu Fall getroffene Entscheidungen und Absicherungen beim Umgang mit personenbezogenen Informationen. Die Reform des Rechtsrahmens stellt einen Schritt in die richtige Richtung dar. Es bestehen jedoch tiefergehende Fragen über die Auswirkung von Tendenzen in einer datengesteuerten Gesellschaft auf Würde, Freiheit des Einzelnen und wirksame Demokratie.

Diese Themen haben technische, philosophische, rechtliche und moralische Implikationen. In dieser Stellungnahme werden einige bedeutende Technologietrends beleuchtet, bei denen es zu einer unannehmbaren Verarbeitung von personenbezogenen Informationen kommen kann oder die das Recht auf Privatsphäre beeinträchtigen können. Als Antwort auf die digitale Herausforderung wird in ihr ein vierstöckiges „großes Datenschutz-Ökosystem" umrissen: eine gemeinsame Anstrengung auf der Grundlage von ethischen Überlegungen.

(1) Zukunftsorientierte Regelung der Datenverarbeitung und Respektierung der Rechte auf Privatsphäre und Datenschutz.
(2) Rechenschaftspflichtige Verantwortliche, die die Verarbeitung von personenbezogenen Informationen bestimmen.
(3) Privatsphärenbewusste Entwicklung und Auslegung von Datenverarbeitungsprodukten und -dienstleistungen.
(4) Menschen mit gestärkter Handlungskompetenz

Der Europäische Datenschutzbeauftragte möchte zu einer offenen und informierten Diskussion innerhalb und außerhalb der EU anregen, an der die Zivilgesellschaft, Produktdesigner, Unternehmen, Gelehrte, Behörden und Gesetzgeber teilnehmen. Der neue EU-Datenschutzethikrat, der beim EDSB eingerichtet wird, trägt dazu bei, einen neuen digitalen Ethos zu definieren, mit dessen Hilfe die Vorteile von Technologie für Gesellschaft und Wirtschaft auf eine Art und Weise besser verwirklicht werden können, die die Rechte und Freiheit des Einzelnen bestärkt.

INHALTSVERZEICHNIS

1. Daten überall: Tendenzen, Gelegenheiten und Herausforderungen

Es werden mehr und mehr personenbezogene Informationen auf immer undurchsichtigere und komplexere Art und Weise erhoben und verarbeitet. Angesichts des fortschreitenden Einsatzes von Computern bei Unternehmen und Behörden in den 80er Jahren des vergangenen Jahrhunderts verstärkte sich die Überzeugung, dass der Einzelne durch die Praktiken mächtiger Regierungen und Unternehmen bei der Verarbeitung von personenbezogenen Daten unter Bedrohung von Grundrechten und Grundfreiheiten auf den Status eines reinen Datensubjekts reduziert wird. Das Unterscheidungsmerkmal der derzeitigen Welle von integrierter Informations- und Kommunikationstechnologie ist ihre Allgegenwärtigkeit und ihre Macht.

Einem Bericht aus dem vergangenen Jahr zufolge gibt es mehr angeschlossene Geräte auf der Welt als Menschen[1]. Erhöhungen bei Prozessorkapazität[2], Speicherkapazität und Übertragungsbandbreite bedeuten, dass die Zahl der technischen Auflagen bei der Verarbeitung von personenbezogenen Informationen fortschreitend geringer wird. Es wird davon ausgegangen, dass das „Internet der Dinge“ und die Analyse von Big Data mit künstlicher Intelligenz, der maschinellen Verarbeitung natürlicher Sprache und biometrischen Systemen verschmelzen, um Anwendungen mit Maschinenlernfähigkeit im Dienste hochentwickelter Geheimdienstinformationen zu ermöglichen. Der Staat und Unternehmen sind in der Lage, vom reinen „Daten-Mining“ zum „Reality-Mining“ überzugehen, das sich in tägliche Erfahrungen, Kommunikationen und sogar in Gedanken einschleicht[3]. Während sich unsere Gesellschaft auf die Anforderungen des digitalen Markts einstellt, gibt es erneut Bemühungen, kleinen Kindern das Programmieren beizubringen[4]. Die Nutzung dieser Tendenzen in einem Sektor, in dem die EU zwar führend im Verbrauch ist, aber beim Anbieten von Diensten hinterherhinkt, ist ein Thema, das in der Strategie der Kommission für den digitalen Binnenmarkt immer wieder anklingt[5].

Diese Tendenzen und viele der heute verwendeten Konzepte sind trotz ihrer Gängigkeit vage und überlappen sich gegenseitig. Zur Anregung einer Debatte möchten wir auf spezifische Tendenzen aufmerksam machen, aus denen sich, aus unserer Sicht zwar nicht erschöpfend, die wichtigsten ethischen und praktischen Fragen für die Anwendung von Datenschutzprinzipien ergeben.

1.1 Big Data

Der Begriff „Big Data“[6] bezieht sich auf die Praxis des Kombinierens immens großer Volumen von Informationen aus verschiedenen Quellen und ihrer Analyse, häufig unter Anwendung von selbstlernenden Algorithmen, als Grundlage der Entscheidungsfindung. Diese Informationen sind nicht immer personenbezogen: sensorgenerierte Daten zur Überwachung von Phänomenen in der Natur oder der Atmosphäre wie Wetter oder Umweltverschmutzung oder zur Überwachung technischer Aspekte von Herstellungsverfahren beziehen sich nicht auf „eine bestimmte oder bestimmbare Person“[7]. Einer der größten Vorteile von Big Data für Unternehmen und Behörden leitet sich jedoch aus der kollektiven und einzelpersonenbezogenen Überwachung von *menschlichem* Verhalten her und beruht auf ihrem Prognosepotenzial[8].

Ein Ergebnis ist die Entstehung eines Ertragsmodells für Internet-Firmen, das auf der Nachverfolgung von Online-Aktivität beruht, um den wirtschaftlichen Wert von

Transaktionen für Dienstanbieter zu optimieren, und zwar nicht nur was gezielte Werbung angeht, sondern auch im Zusammenhang mit Versicherungsbedingungen und -prämien, Darlehen und Vertragsbeziehungen. Bei dem vom Wettbewerb geprägten Streben um die Aufmerksamkeit der Nutzer ist sich kaum jemand des Ausmaßes dieser Nachverfolgung bewusst[9]. Derartige „Big Data“ sollten als personenbezogen klassifiziert werden, selbst wenn Anonymisierungstechniken zur Anwendung gekommen sind: Der Rückschluss auf die Identität einer Person durch das Kombinieren von angeblich „anonymen“ Daten mit anderen Datensätzen, einschließlich öffentlich, beispielsweise auf sozialen Medien, zugänglicher Informationen, wird immer einfacher[10]. Wenn mit diesen Daten gehandelt wird, insbesondere über Landes- und Gerichtsbarkeitsgrenzen hinweg, ist die Frage nach der Verantwortung für die Verarbeitung der Informationen nicht mehr so leicht zu beantworten; Feststellung und Durchsetzung von Verantwortlichkeit gemäß dem Datenschutzrecht sind problematisch, besonders da keine internationalen Normen vorliegen.

1.2 „Internet der Dinge“

Viele Geräte, die mit dem Internet verbunden sind, wie Smartphones, Tablets, Geldautomaten und Check-In-Automaten am Flughafen, gehören bereits zum Alltag. Konnektivität ist, Prognosen zufolge, im Jahr 2020 mit 25 Milliarden angeschlossenen Geräten (im Vergleich zu 4,8 Milliarden im Jahr 2015), von Telemedizin bis zur Fahrzeugtechnik, von intelligenten Zählern bis zu einem ganzen Spektrum an neuen stationären und mobilen Geräten zur Verwirklichung von intelligenten Städten, die Norm[11].

Diese Sensoren stellen unmittelbare und detaillierte Informationen zur Verfügung, die heute über statistische Ämter und Erhebungen zwar noch nicht erhalten werden können, aber nicht unbedingt präziser sind und möglicherweise sogar irreführend sein können[12]. Die schätzungsweise 1,8 Milliarden Anbindungen von Maschine zu Maschine im Automobilbereich, von denen bis 2022 ausgegangen wird, könnten die Zahl der Unfälle sowie Umweltverschmutzung reduzieren, die Produktivität erhöhen und das Leben von betagten und behinderten Menschen unabhängiger gestalten[13]. "Tragbare Geräte“ wie Kleidung und Armbanduhren verarbeiten personenbezogene Informationen wie andere angeschlossene Geräte. Sie werden in der Lage sein, Blutgerinnsel zu erfassen sowie körperliche Fitness und Wundheilung zu überwachen; angeschlossene Gewebe könnten Schutz vor extremen Umgebungsbedingungen bieten, denen man beispielsweise bei der Brandbekämpfung begegnet. Mit diesen Geräten werden personenbezogene Daten direkt in das Cloud-Speichernetzwerk hochgeladen, gelangen auf diesem Weg in die sozialen Netzwerke und werden unter Umständen öffentlich rundgesendet, wobei Nutzer identifiziert und das Verhalten von Einzelpersonen und Menschenmengen und die von diesen zurückgelegten Wege nachverfolgt werden können[14].

Wie mit diesen Informationen umgegangen wird, könnte sich nicht nur auf die Privatsphäre der Nutzer der Geräte, einschließlich des Nutzungsortes am Arbeitsplatz, sondern auch auf die Rechte anderer auswirken, die von dem Gerät beobachtet und aufgenommen werden. Auf tatsächliche Diskriminierung weist zwar nur wenig hin, aber es steht außer Zweifel, dass das große Volumen an personenbezogenen Informationen, die vom „Internet der Dinge“ gesammelt werden, als Mittel zur Maximierung von Erträgen durch eine stärker personenbezogene Preisgestaltung in Übereinstimmung mit beobachtetem Verhalten, besonders im Krankenversicherungssektor, von großer Bedeutung ist[15]. Andere domänenspezifische Regeln werden ebenfalls hinterfragt; dies gilt beispielsweise für Geräte,

die zwar Gesundheitsdaten verarbeiten, aber technisch nicht als medizinische Geräte zu klassifizieren sind und nicht in den Geltungsbereich der Regelung fallen[16].

1.3 Ambient Computing

Ambient Computing oder unsichtbare rechnergestützte Informationsverarbeitung bezieht sich auf eine Schlüsseltechnologie, auf der das „Internet der Dinge“ beruht. Eine der naheliegendsten Anwendungen ist das „intelligente Heim“ oder das „intelligente Büro“, das aus Geräten mit eingebauter moderner Informationsverarbeitungskapazität besteht, mit denen man sich Energieeinsparungen und besser informierte Verbraucher verspricht, die in der Lage sind, ihren Verbrauch ferngesteuert zu beeinflussen (obwohl dies von der Selbständigkeit des Bewohners gegenüber dem Vermieter oder dem Gebäudeverwalter abhängig wäre). Es muss eindeutig sein, wer für den Zweck und die Mittel der Verarbeitung der personenbezogenen Daten, die von Ambient-Computing-Anwendungen betroffen sind, verantwortlich ist, und zwar nicht nur für den Schutz der Grundrechte des Einzelnen, sondern auch für die Haftungszuweisung, damit die Erfüllung von Sicherheitsanforderungen des Gesamtsystems gewährleistet ist.

1.4 Cloud-Computing

Unter Cloud-Computing versteht man die zentrale Technologie, die fortschrittliche Analyse- und Mining-Kapazitäten, die Erhebung und Analyse von Big Data sowie den Fluss von Daten vom „Internet der Dinge“ ermöglicht und derzeit von ungefähr einem Fünftel aller EU-Bürger und Unternehmen in der EU eingesetzt wird[17]. Es ermöglicht die Konzentration von Daten der zahllosen Geräte des „Internet der Dinge“ und beruht auf der Verfügbarkeit und Konnektivität enormer Datenvolumen in groß angelegten Speicher- und Verarbeitungseinrichtungen in der ganzen Welt[18]. Schätzungen zufolge würde sich das EU28 BIP durch eine ausgedehntere Nutzung von Cloud-Computing[19] durch den privaten und den öffentlichen Sektor potenziell um insgesamt €449 Milliarden erhöhen (0,71% des EU-BIP insgesamt).

Die Kontrolle über personenbezogene Informationen liegt oft zum Teil beim Kunden und zum Teil beim Cloud-Dienstanbieter, und die Verantwortung für die Datenschutzpflichten ist nicht immer eindeutig. Das kann bedeuten, dass der Schutz in der Praxis ungenügend ist. Diese Verpflichtungen sind von dem **physischen Datenspeicherort** unabhängig. **Außerdem** ist es möglich, dass sich die Cloud-Computing-Infrastruktur ihrerseits, obwohl es sich nur um eine die Geschäftsanwendungen unterstützende Hintergrundtechnologie handelt, zu einer kritischen Infrastruktur entwickeln und das Ungleichgewicht in Marktmacht verstärken kann, da 30% von Unternehmen in letzter Zeit von Problemen beim Abmelden oder beim Wechsel von Dienstanbietern berichtet haben[20].

1.5 Von personenbezogenen Daten abhängige Geschäftsmodelle

Dank dieser Technologien können in neuen Geschäftsmodellen, bei denen es auf Informationen ankommt, die nicht nur aus der Bereitstellung von Dienstleistungen, sondern auch aus anderen Quellen wie der Präsenz in sozialen Medien hervorgehen, Risiko und Kreditwürdigkeit beurteilt und Erträge maximiert werden. Ein bekanntes derzeitiges Geschäftsmodell wird durch Plattformen dargestellt, die Verkäufer mit Käufern verbinden und die gemeinsame Nutzung und Neuverteilung von Produkten, Dienstleistungen, Fähigkeiten und Wertanlagen ermöglichen. Diese Plattformen, die oft als „Share Economy“, „kollaborativer Konsum“ oder Online- und mobile Peer-to-Peer-Geschäftsplattformen

bezeichnet werden,[21] können klassische Effizienzsteigerungen bieten, den Wettbewerb in einem Markt verstärken und Abfallaufkommen reduzieren. Schätzungen zufolge wird sich ihr globaler Wert in den kommenden Jahren von $26 auf $110 Milliarden vervierfachen[22]. Derartige datenorientierte Geschäftsmodelle generieren schon jetzt enorme Erträge bei Fahrgemeinschaften, der Vermietung von Häusern, in der Finanztechnologie und bei Sozialdarlehen. Aus Umfragen geht hervor, dass Verbraucher ihre größere Erschwinglichkeit und Praktikabilität schätzen[23].

Die Valuta derartiger Plattformen ist üblicherweise Nutzerreputation, Begutachtung durch Gleichgestellte und Identitätsverifizierung. Dies kann potenziell als Verbesserung von Transparenz und Verantwortlichkeit betrachtet werden, jedoch nicht unbedingt in Bezug auf den Plattformanbieter selbst. Großen Teilnehmern auf diesen Märkten ist vorgeworfen worden, dass sie angeblich reputationsbezogene Daten gerade den einzelnen Nutzern vorenthalten, auf die sich die Informationen beziehen. Es besteht die große Gefahr, dass Personen aufgrund von falschen Daten, die sie nicht anfechten können oder deren Löschung sie nicht fordern können, der Zugang auf Dienstleistungen auf Reputationsgrundlage verwehrt werden könnte. Auch das Vertrauen auf Daten aus zahlreichen Quellen stellt das EU-Rechtsprinzip der Datenminimierung in Frage. Das Ausmaß der künftigen Auswirkungen dieser und zukünftiger Geschäftsmodelle auf Technologiebasis auf den Einzelnen und die Gesellschaft muss sorgfältig überdacht werden[24].

1.6 Flugroboter und autonome Fahrzeuge

Flugroboter, auch semi-autonome Flugzeuge genannt, sind derzeit in der Hauptsache im militärischen Einsatz, werden aber zunehmend für Überwachung, Kartografierung, Transport, Logistik und für die öffentliche Sicherheit wie in der Waldbrandbekämpfung eingesetzt[25]. Fotografien, Videos und andere personenbezogene Daten, die von Flugrobotern aufgenommen bzw. erhoben werden, können über Telekommunikationsnetze ausgetauscht werden. Durch ihren Einsatz besteht die Gefahr von ernstzunehmenden Angriffen auf die Privatsphäre und einer Bedrohung der freien Meinungsäußerung. Es stellt sich die Frage, wie ihre Auslegung und Verwendung effektiv geregelt werden kann, so dass betroffene Personen ihre Rechte auf Zugang zu Daten, die von diesen Maschinen gesammelt worden sind, ausüben können.

Am Boden leiten autonome Fahrzeuge und fahrerlose Autos den Wandel des Einsatzes und der Organisierung des Personenverkehrs ein, wodurch sich der Unterschied zwischen privaten und öffentlichen Verkehrsmitteln möglicherweise verwischt. Schätzungen zufolge werden sich bis 2035 12 Millionen voll autonome und 18 Millionen teilweise autonome Fahrzeuge auf europäischen Straßen befinden, wobei Europa zu den Vorreitern in dieser Entwicklung gehören wird[26]. Die die Fahrzeuge steuernden Algorithmen werden Entscheidungen treffen, die sich unmittelbar auf die körperliche Unversehrtheit und, beispielsweise im Falle der bei einem unvermeidbaren Zusammenprall einprogrammierten Wahl, sogar auf das Überleben der Betroffenen auswirken können. Abgesehen davon, dass es offensichtlich eindeutig klar sein muss, wer für Datenkontrolle und Datensicherheit verantwortlich ist und haftet, stellen sich bei diesen Anwendungen eine Reihe von ethischen Fragen.

1.7 Tendenzen, die möglicherweise größere, längerfristige Auswirkungen haben

Das 3D-Bioprinting von organischem Material, bei dem zum Niederlegen von aufeinanderfolgenden Reihen lebender Zellen Patientenzellkopien und „Bio-Bandagen“ aus

Kollagen (d. h. sensible Daten nach EU-Recht) verwendet werden, ist Schätzungen zufolge bald einsatzfähig[27]. Dadurch wären patientenspezifische Körperteile leichter erhältlich, was besonders in ärmeren Teilen der Welt und nach dem Ende von kriegerischen Auseinandersetzungen von enormer Bedeutung wäre. In Bezug auf das Bioprinting stellen sich offensichtlich nicht nur Fragen über Ethik in der Medizin, die Wahrung von geistigem Eigentum und den Verbraucherschutz, sondern auch Fragen über die Geltung der Datenschutzregeln, da beim Bioprinting persönliche und sensible Daten über den Gesundheitszustand des Einzelnen verarbeitet werden.

Künstliche Intelligenz bezieht sich wie Robotertechnik auf ein technologisches Erfordernis für feststehende und mobile autonome Maschinen. Ihre Weiterentwicklung bietet ein ungeheures Potenzial, das weit über ihre derzeitige Anwendung hinausgeht. Computer, die nach dem „Deep Learning"-Verfahren arbeiten, bringen sich selbst Aufgaben bei, indem sie unter Einsatz von (unter anderem) neuronalen Netzen, die wie das menschliche Gehirn zu arbeiten scheinen, umfangreiche Datensätze verarbeiten. Forschung und Wirtschaft arbeiten darauf hin, unüberwachtes Lernen zu verbessern. Schon jetzt sind Algorithmen in der Lage, Sprachen zu verstehen und zu übersetzen, Bilder zu erkennen, Nachrichtenartikel zu schreiben und medizinische Daten zu analysieren[28]. Soziale Medien liefern Unmengen an personenbezogenen Informationen, die praktisch schon von den betroffenen Personen selbst gekennzeichnet sind. Dabei handelt es sich zwar möglicherweise um die neuste einer Reihe von kognitiven Verbesserungen zur Steigerung der Kapazität des menschlichen Gehirns, zu denen Erfindungen wie Papier oder der Abakus gehören oder die Weiterentwicklung von integrierten zu autonomen Maschinen, Robotern, aber es ist an der Zeit, die weiteren Auswirkungen auf den Einzelnen und die Gesellschaft zu berücksichtigen[29].

2. Ein großes Datenschutz-Ökosystem

Die EU hat jetzt die Möglichkeit, allen voran als Erste zu zeigen, wie Regierungen, Gesetzgeber, für die Datenverarbeitung Verantwortliche, Designer, Entwickler und Einzelpersonen besser zusammenarbeiten können, um Rechte zu stärken und die technologische Innovation zu lenken und ihr nicht im Wege zu stehen. Die in Abschnitt zwei beschriebenen Tendenzen haben in den Worten eines Kommentators „den Abstand zwischen dem, was möglich ist, und dem, was rechtlich gestattet ist, vergrößert"[30]. Im Gegensatz zu dem, was zuweilen behauptet wird, stellen der Schutz der Privatsphäre und der Datenschutz kein Hindernis für eine nachhaltige und dynamische digitale Umgebung dar, sondern sind eine Plattform dafür. Bei der Entzauberung derartiger Märchen und als Anlaufstelle für Personen, die sich ernste Sorgen um den Verlust der Kontrolle über ihre personenbezogenen Informationen machen, kommt unabhängigen Datenschutzbehörden wie dem EDSB eine Schlüsselrolle zu[31].

Die nächste Generation personenbezogener Daten ist für die betroffenen Personen wahrscheinlich noch weniger zugänglich. Die Verantwortung für die Gestaltung eines nachhaltigen digitalen Binnenmarkts kann selbstverständlich nicht bei einer einzigen Instanz liegen, aber zwischen den beteiligten Instanzen besteht wie in einem Ökosystem auch eine gegenseitige Abhängigkeit, die einer wirksamen Zusammenarbeit zwischen Entwicklern, Unternehmen und Gesetzgebern im Interesse der betroffenen Personen bedarf. In diesem Abschnitt umreißen wir den Beitrag, der von diesen vier wesentlichen Beteiligten geleistet werden kann.

2.1 Zukunftsorientierte Regelung

Vor nicht allzu langer Zeit haben wir die EU dazu aufgerufen, diesen historischen Moment zu nutzen und einfachere Regeln für den Umgang mit personenbezogenen Informationen zu erlassen, die ihre Relevanz nicht innerhalb einer Generation verlieren[32]. Die Verhandlungen über die Allgemeine Datenschutzverordnung und die Richtlinie für den Datenschutz in Polizei- und Justizbehörden nähern sich ihrem Ende, wonach die Zukunft der Datenschutzrichtlinie für elektronische Kommunikation und der neuen Verordnung darüber, wie Organe und Einrichtungen der EU selbst personenbezogene Daten verarbeiten, bald in den Mittelpunkt der Diskussion rücken wird. Da für das Erheben und Speichern von Daten fast keine wirtschaftlichen Kosten entstehen, wird die Aufgabe der einheitlichen Durchsetzung dieser Regeln zur Vermeidung des „moralischen Risikos" einer übermäßigen Datenverarbeitung den Datenschutzbehörden zufallen[33].

In der Strategie des digitalen Binnenmarkts wird die Verbindung zwischen der Kontrolle großer Datenvolumen und Marktmacht erkannt. Darin kommt die Überzeugung zum Ausdruck, dass eine größere Kohärenz unter den Gesetzgebern nötig ist, worauf wir bereits in unserer vorläufigen Stellungnahme zu „Datenschutz und Wettbewerbsfähigkeit im Zeitalter von Big Data" von 2014 hinwiesen. Die EU verfügt bereits über das Instrumentarium zur Behebung des Machtgefälles im digitalen Markt: die derzeitigen Kartellverfahren der Europäischen Kommission sind ein Beweis für die Vormachtstellung von Mobilgeräten für den Internet-Zugang. Möglich ist eine gesamtheitlichere Durchsetzung innerhalb des bestehenden gesetzlichen Rahmens wie beispielsweise über eine EU-Clearingstelle, so dass Aufsichtsbehörden darüber entscheiden können, ob Einzelfälle zu Fragen über die Beachtung von Wettbewerbs-, Verbraucher- und Datenschutzregeln führen können. Beispiele:

- Durch das Erfordernis einer größeren Transparenz der Kosten, ob in bar oder anderweitig entrichtet, für einen Dienst können Wettbewerbssachen verdeutlicht und ihre Analyse erleichtert werden[34], und

- Erfassung von ungerechten Preisunterschieden auf der Grundlage von schlechter Datenqualität und von ungerechten Profilierungen und Korrelationen[35].

Ein engerer Dialog zwischen Behörden aus unterschiedlichen Sektoren könnte zu der Bildung von globalen Partnerschaften führen, deren Notwendigkeit zunehmend erkannt wird und die eine Art von Gemeinschaftsbereich offener Daten schaffen können, in dem Daten und Ideen wie beispielsweise Statistiken und Landkarten mit geringerem Überwachungsrisiko frei fließen können, zur Verfügung stehen und im öffentlichen Interesse ausgetauscht werden können, so dass der Einzelne mehr Einfluss über Entscheidungen hat, die ihn betreffen[36].

2.2 Rechenschaftspflichtige Verantwortliche

Zur Rechenschaftspflicht oder Verantwortlichkeit gehört das Vorsehen von internen Richtlinien und Kontrollsystemen, die für die Beachtung der Regeln sorgen und insbesondere unabhängigen Aufsichtsbehörden relevante Beweise zur Verfügung stellen.

Wir haben für die Abschaffung von Bürokratie im Datenschutzrecht durch Reduzierung von unnötiger Dokumentation plädiert, damit so viel Raum wie möglich für mehr verantwortliche Initiative seitens der Unternehmen, unterstützt durch die Weisungen von Datenschutzbehörden, vorhanden ist. Der Grundsatz, nach dem personenbezogene Daten nur so verarbeitet werden sollten, wie es dem/den spezifischen Zwecke/n entspricht, für den/die

sie erhoben wurden, ist für die Beachtung der legitimen Erwartungen der betroffenen Personen wesentlich. Verhaltensrichtlinien, Audits, Zertifizierung und eine neue Generation von Vertragsbedingungen und verbindlichen Unternehmensregeln können beispielsweise dazu beitragen, eine solide Vertrauensbasis für den digitalen Markt zu schaffen. Jene, die für den Umgang mit personenbezogenen Informationen verantwortlich sind, sollten sich viel dynamischer und proaktiver verhalten und sich von der so genannten „Black Box"-Tendenz der Geheimhaltung und Undurchsichtigkeit von Geschäftspraktiken distanzieren, während sie gleichzeitig mehr Transparenz von Kunden verlangen[37].

2.3 Privatsphärenbewusste Entwicklung

Menschliche Innovation ist schon immer das Ergebnis von Aktivitäten bestimmter gesellschaftlicher Gruppen und spezifischer Umstände gewesen und spiegelte üblicherweise die im jeweiligen Zeitalter geltenden gesellschaftlichen Normen wieder[38]. Technologische Design-Entscheidungen sollten jedoch unsere Werte und Grundrechte unterstützen und nicht unser Zusammenleben mit den anderen Mitgliedern unserer Gesellschaft und die Struktur unserer Gemeinschaft diktieren.

Die EU sollte technologische Verfahren und Methodologien entwickeln und fördern, dank derer Datenverarbeitungstechnologien implementiert werden können, bei denen die Würde und die Rechte des Einzelnen voll umfänglich gewährt werden. System- und Software-Ingenieure müssen bei neuen Produkten und Dienstleistungen in Design-Phasen und Technologien die Prinzipien des eingebauten Datenschutzes verstehen und besser zur Anwendung bringen. Verantwortlichkeit muss durch mehr Forschung und Entwicklung bei Verfahren und Instrumenten untermauert werden, um präzise Audits zu gewährleisten und zu bestimmen, dass die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter die Regeln beachten, wie etwa durch „Markieren" jeder personenbezogenen Dateneinheit mit „Metadaten", die Datenschutzanforderungen beschreiben.

Der Einzelne, der seine Privatsphäre und Freiheit durch Anonymität wahren möchte, sollte durch technische Lösungen dazu in die Lage versetzt werden. Die EU sollte die Konzipierung und Implementierung von Algorithmen fördern, die zum Schutz des Einzelnen die Identität von Personen geheimhalten und Daten aggregieren, und dabei gleichzeitig die Vorhersagekraft der Daten nutzbringend einsetzen[39].

Wir müssen heute den Grundstein für die Bewältigung dieser Aufgaben legen, indem wir Entwickler und Datenschutzexperten aus unterschiedlichen Bereichen in weiten Netzwerken wie dem IPEN (Schutz der Privatsphäre im Internet Engineering Netzwerk) zusammenführen, was zu einem ergiebigen interdisziplinären Austausch von Ideen und Ansätzen führt.

2.4 Menschen mit gestärkter Handlungskompetenz

Eine „Prosumer"-Umgebung (Pro-ducer/Con-sumer - Produzent/Verbraucher)

Der Einzelne ist nicht einfach ein passives Subjekt, das Rechtsschutz gegen Ausbeutung benötigt. Die oben beschriebenen digitalen Trends bieten auch positive Möglichkeiten zur Stärkung der Rolle des Individuums. Beispielsweise ist heute ein Produzent von Inhalt und Diensten auch gleichzeitig ein Verbraucher von Inhalt und Diensten und gilt in zunehmendem Maße zusammen mit Dienstanbietern als gemeinsam für die Verarbeitung von personenbezogenen Daten verantwortlich, es sei denn, es ist ein reiner „Hausgebrauch" beabsichtigt[40] (zur Beschreibung dieser Entwicklung entstand das Konzept des „Prosumers"

[41]). In der Zwischenzeit bieten virtuelle Währungen Nutzern Anonymität und die Umgehung der Verifikation von Transaktionen durch Dritte, wodurch die Transaktionskosten beim Zahlen für Waren und Dienstleistungen aus dem Ausland gesenkt werden. Andererseits macht sich der Einzelne aufgrund der Anonymität und der Tatsache, dass Transaktionen mit virtuellen Währungen zwischen unterschiedlichen Rechtsordnungen (oder, so könnte man argumentieren, in *keiner* Rechtsordnung) stattfinden, zur Zielscheibe für Betrüger und kriminelle Marktteilnehmer, die sich nur schwer fassen und ermitteln lassen. Abgesehen von den Pflichten von Behörden, Unternehmen und Technikern sind auch Bürger dazu aufgerufen, ob online oder nicht, bewusste, geistesgegenwärtige, kritische und informierte Entscheidungen zu treffen[42].

Einwilligung

Im Gegensatz zu der herkömmlichen Meinung kann darüber hinaus nicht jedes menschliche Verhalten durch Wirtschaftsprinzipien, die davon ausgehen, dass Menschen völlig rationale Wesen sind und für wirtschaftliche Anreize empfänglich sind, erklärt werden[43]. Dies ist für die zukünftige Rolle relevant, die der Einwilligung des Betroffenen zu der Verarbeitung von personenbezogenen Informationen über ihn zukommt. Nach EU-Recht ist Einwilligung nicht die einzige legitime Grundlage für den größten Teil der Datenverarbeitung. Selbst da, wo Einwilligung eine wichtige Rolle spielt, sind für die Verarbeitung Verantwortliche nicht von ihrer Pflicht befreit, für den Zweck ihrer Datenverarbeitung Rechenschaft abzulegen, insbesondere dann, wenn es um eine verallgemeinerte Einwilligung zu der Verarbeitung für die verschiedensten Zwecke geht.

Kontrolle und Daten-„Inhaberschaft“

Der Einzelne muss in der Lage sein, sich über Fehler und ungerechte Behandlung zu beschweren, die sich aus der Logik ergeben, die von Algorithmen zur Bestimmung von Annahmen und Vorhersagen eingesetzt wird. Beispielsweise ergab sich aus einer Studie von fast 3000 Kreditauskünften für 1000 Verbraucher in den USA, dass 26 Prozent davon „erhebliche“ Fehler aufwiesen, die so schwerwiegend waren, dass sie sich auf die Kreditwürdigkeit der jeweiligen Verbraucher und damit auf die Kosten für den Zugang zu Krediten auswirkten[44].

Daten werden oft als eine Ressource angesehen, mit der gehandelt werden kann wie mit Öl gehandelt wird, und zwar idealerweise durch gleichermaßen gut informierte Transaktionsparteien[45]. Kunden erhalten für ihre personenbezogenen Informationen, mit denen gehandelt wird, keine gerechte Vergütung, und manche haben sich für ein Dateninhaberschaftsmodell ausgesprochen. Eine absolute Kontrolle über personenbezogene Daten lässt sich jedoch nur schwer garantieren - es bestehen immer noch andere Erwägungen wie etwa das öffentliche Interesse und die Rechte und Freiheiten anderer. Kontrolle ist notwendig, aber nicht ausreichend[46]. Menschenwürde ist immer jedoch gleichbleibend, und gemäß EU-Recht kann die Analogie zu Inhaberschaft oder Eigentum als solches nicht auf personenbezogene Informationen angewandt werden, da sie in enger Verbindung zu der Persönlichkeit des Einzelnen stehen. Im EU-Datenschutzrecht ist der Verzicht auf dieses Grundrecht nicht vorgesehen.

Ein alternatives Verfahren, mit dem Betroffenen mehr Kontrolle über ihre Daten gegeben wird und darüber, wer Zugang zu ihnen hat und für welchen Zweck, wäre möglicherweise die Verwendung von personenbezogenen Datenspeichern oder so genannten „Data Vaults„“[47]. Das Konzept eines solchen „personenbezogenen Speichers“ erfordert Sicherheitsmaßnahmen,

die gewährleisten, dass nur vom Betroffenen Bevollmächtigte Zugang zu den Daten haben und dann nur zu den Teilen, für die die Bevollmächtigung gilt. Am wirksamsten wären personenbezogene Datenspeicher bei aktuellen und ständig aktualisierten Informationen wie etwa Geodaten oder Lebenszeichen. Über die technischen Sicherungsmaßnahmen hinaus wären Datennutzer dazu verpflichtet, die Regeln in Bezug auf gemeinsame Nutzung und Gebrauch von Daten zu respektieren. Der Wettbewerb und die Möglichkeit, zu einem anderen Dienst zu wechseln, ist die wirksamste Waffe des Verbrauchers, um den ihm zur Verfügung stehenden Dienstleistungsmarkt zu beeinflussen. Es hat sich herausgestellt, dass die Gewährleistung der Übertragbarkeit von Anschlüssen, einschließlich Identifikatoren und Kontaktinformationen, die Konkurrenz ungeheuer belebt und Verbraucherpreise wirksam gesenkt hat, als der Telekom-Markt liberalisiert wurde. Datenübertragbarkeit, d. h. die tatsächliche und praktische Möglichkeit des Transfer der meisten eigenen Daten von einem Dienstanbieter zu einem anderen, ist ein guter Ausgangspunkt für die Schaffung der Bedingungen dafür, dass der Verbraucher eine echte Wahl hat.

3. Würde im Zentrum eines neuen digitalen Ethos

Die Bausteine dieses digitalen Ökosystems müssen auf einem ethischen Fundament ruhen. Nach Ansicht des EDSB könnten größere Achtung der Menschenwürde und ihre Sicherung das Gegengewicht zu der allgegenwärtigen Überwachung und den ungleichen Kräfteverhältnissen, denen sich der Einzelne gegenübersieht, bilden. Dies sollte im Zentrum eines neuen digitalen Ethos stehen.

3.1 Würde und Daten

Im Anschluss an die industrielle Revolution im 18. und 19. Jahrhundert war die Menschenrechtsbewegung bestrebt, durch die Ausräumung der Hindernisse, die der Respektierung des Einzelnen im Wege stehen, das Wohl des Menschen sicherzustellen. Mit ihrer Charta der Grundrechte und nach der Allgemeinen Erklärung der Menschenrechte und der Europäischen Menschenrechtskonvention hat die Europäische Union nun die Unantastbarkeit der Menschenwürde als Ausgangspunkt gewählt. Die Würde des Menschen ist nicht nur an sich schon ein Grundrecht, sondern ist auch der Ursprung nachfolgender Freiheiten und Rechte, einschließlich des Rechts auf eine Privatsphäre und den Schutz von personenbezogenen Daten[48]. Eine Verletzung der Menschenwürde wäre beispielsweise die Vergegenständlichung, d. h. eine Person wird als Werkzeug für die Zwecke anderer eingesetzt[49]. Die Privatsphäre ist Bestandteil der Menschenwürde, und das Recht auf Datenschutz wurde ursprünglich in den 70er und 80er Jahren des 20. Jahrhunderts als Mittel konzipiert, um dem möglichen Abbau von Privatsphäre und Menschenwürde durch die großangelegte Verarbeitung von personenbezogenen Daten entgegenzuwirken. Die Grundlage für das Recht auf „informationelle Selbstbestimmung“ in Deutschland ist das Recht auf Menschenwürde und auf die freie Entfaltung der Persönlichkeit wie in Artikel 1 und 2 des Grundgesetzes für die Bundesrepublik Deutschland festgelegt[50].

Zu Beginn des 21. Jahrhunderts ist es jedoch erforderlich, dass der Einzelne viel mehr personenbezogene Informationen über das Internet weitergibt, um am sozialen, administrativen und geschäftlichen Leben teilnehmen zu können, wobei immer weniger die Möglichkeit eines Ausstiegs besteht. Da alle Aktivitäten möglicherweise immer online stattfinden, ist der Grundsatz einer freien und informierten Einwilligung kaum noch haltbar. Von Minute zu Minute fallen „digitale Brosamen“, die kombiniert zur Klassifizierung von Personen in Echtzeit verwendet werden, um mehrfache und zuweilen sich widersprechende

Profile zu erstellen. Diese Profile können ohne Wissen der Betroffenen innerhalb von Mikrosekunden in Umlauf gebracht und als Grundlage von wichtigen, sich auf sie auswirkenden Entscheidungen genutzt werden.

Bei Profilen, die zur Vorhersage von menschlichen Verhaltensweisen dienen, besteht die Gefahr der Stigmatisierung: bestehende Stereotypen, soziale und kulturelle Segregation und Ausgrenzung werden verstärkt[51], da eine derartige „kollektive Intelligenz" die Wahlmöglichkeiten des Einzelnen und die Gleichberechtigung zunichte macht. Es könnte sich herausstellen, dass derartige „Filterblasen" oder „persönliche Hallräume" gerade die Kreativität, die Innovation und die Möglichkeiten der freien Meinungsäußerung und der Versammlungsfreiheit ersticken, dank derer digitale Technologien sich überhaupt entwickeln konnten.

Zwischenzeitlich wird ein mit Befürchtungen hinsichtlich der „Sicherheit" begründeter ständiger Ausnahmezustand dazu genutzt, die vielschichtigen Schnüffeltechniken zur Überwachung der Aktivitäten des Einzelnen zu rechtfertigen[52]. Es bedarf einer längerfristigen Perspektive der Auswirkungen auf Gesellschaft und Verhalten insgesamt, um dieses sich immer weiter zusammenziehende Überwachungsnetz zu verstehen.

Gemeinsam mit Drittländern muss die EU kompromisslos überprüfen, wie sichergestellt werden kann, dass diese Werte nicht nur auf dem Papier respektiert werden, während sie im Cyberspace eigentlich bedeutungslos sind. Vor der Übernahme dieser Technologien en masse hat insbesondere die EU jetzt ein „kritisches Zeitfenster", um die Werte in digitalen Strukturen zu verankern, die unsere Gesellschaft definieren werden[53]. Dazu muss neu beurteilt werden, ob die potenziellen Vorteile der neuen Technologien tatsächlich von der Erhebung und Analyse der persönlich identifizierbaren Informationen von Milliarden von Menschen abhängig sind. Eine solche Beurteilung könnte Entwickler dazu zwingen, Produkte zu schaffen, mit denen riesige Volumen von ungeordneten Informationen in Echtzeit anonymisiert werden können, so dass die Vereinzelung von Datensubjekten nicht oder nur schwer möglich ist

Es ist bereits eine anerkannte Tatsache, dass die Verarbeitung von bestimmten Informationen, wie etwa genetischen Daten, nicht nur gesetzlich geregelt werden muss, sondern auch beispielsweise durch Ethikausschüsse auf allgemeinere gesellschaftliche Fragen hin zu überprüfen ist. Genetische Daten beziehen sich per definitionem nicht nur auf eine einzige Person, sondern auch auf ihre Vorfahren und ihre Nachkommen. Genetische Daten dienen nicht allein zur Aufdeckung von Verwandtschaftsverhältnissen; aus Elementen in den Genen eines Menschen lassen sich auch Informationen über seine Eltern und seine Kinder ableiten, was zu Entscheidungen der für die Verarbeitung Verantwortlichen führt, die ihre Chancen im Leben noch vor der Geburt beeinflussen. Die potenzielle Konzentrierung von personenbezogenen genetischen Daten in den Datenbanken einiger weniger großer Marktteilnehmer wirkt sich sowohl auf Marktwirtschaften als auch auf die betroffenen Personen aus. Zunehmende Abhängigkeit von einem globalen System zur Erhebung und Analyse eines permanenten Datenstroms könnte dazu führen, dass Gesellschaft und Wirtschaft anfälliger für noch nie dagewesene Sicherheitslücken und kriminelle Angriffe sind.

Der bestehende Rahmen könnte versagen, wenn wir der Zukunft nicht mit innovativem Denken begegnen. Forderungen werden immer lauter und die Notwendigkeit wird immer dringender, die betroffene Person nicht einfach als Verbraucher oder Nutzer, sondern als Individuum zu betrachten. Wirklich unabhängigen Datenschutzbehörden kommt eine

ausschlaggebende Rolle dabei zu, eine Zukunft zu verhindern, in der Menschen durch Algorithmen und ihre kontinuierlichen Variationen bestimmt werden. Sie müssen über geeignete Werkzeuge verfügen, damit sie ihrer „Sorgfaltspflicht“ gegenüber dem Einzelnen und seiner Würde im Internet nachkommen können. Herkömmliche Privatsphären- und Datenschutzkonzepte und -prinzipien wie in den Bereichen Arbeit und Gesundheit waren zum Schutz der Menschenwürde bereits ethisch nuanciert. Durch die heute zu beobachtenden Tendenzen wurde jedoch ein völlig neues Kapitel aufgeschlagen; es muss geprüft werden, ob die Grundsätze stark genug für das digitale Zeitalter sind[54]. Der Begriff „personenbezogene Daten“ selbst ändert sich wahrscheinlich radikal, da es anhand von Technologie mehr und mehr möglich ist, den Einzelnen auf der Grundlage von angeblich anonymen Daten kenntlich zu machen. Maschinenlernen und die Verschmelzung von menschlicher und künstlicher Intelligenz werden zudem die Konzepte der Rechte und Verantwortung, die der Einzelne hat, untergraben.

3.2 Ein europäischer Ethik-Beirat

Hiermit soll die Zukunft nicht schwarzgemalt werden. Es finden bereits Diskussionen in juristischen, politischen, wirtschaftlichen, sozialen, wissenschaftlichen und sogar religiösen Kreisen statt[55]. Rein auf wirtschaftlichen Gewinn oder die Sicherheitsüberwachung ausgerichtete simplistische Ansätze bringen uns genauso wenig weiter wie die übermäßig einschränkende Anwendung bestehender Gesetze und Regelungen, in denen Innovation und Fortschritt ersticken. Der EDSB schlägt daher eine gründliche, breit gefasste und multidisziplinäre Analyse vor, bei der Empfehlungen erarbeitet werden und auf deren Grundlage eine gesellschaftsweite Debatte darüber stattfinden kann, wie sich eine demokratische Gesellschaft der technologischen Herausforderung stellt.

Die EDSB-Strategie[56] zielt darauf ab, einen ethischen Ansatz für den Datenschutz zu entwickeln, bei dem berücksichtigt wird, dass „Machbarkeit, Nützlichkeit und Rentabilität nicht mit Nachhaltigkeit gleichzusetzen sind“, und bei dem „die Rechenschaftspflicht im Gegensatz zur mechanischen Konformität mit dem Wortlaut des Gesetzes“ betont wird. Unsere Absicht ist es, über die Gemeinschaft von EU-Beamten, Anwälten und IT-Experten hinauszugehen und eminente Persönlichkeiten mit einzubinden, die in der Lage sind, die mittel- bis langfristigen Auswirkungen von technologischem Wandel und regulatorischen Antworten zu beurteilen. Wir als unabhängiges EU-Organ werden in den kommenden Monaten eine externe Beratergruppe für die ethische Dimension des Datenschutzes einrichten, die die Beziehungen zwischen Menschenrechten, Technologie, Märkten und Geschäftsmodellen im 21. Jahrhundert untersucht.

Unser Ethik-Beirat wird aus einer exklusiven Gruppe von Persönlichkeiten aus den Gebieten Ethik und Philosophie, Soziologie, Psychologie, Technologie und der Wirtschaftswissenschaft bestehen; unterstützt wird diese Gruppe nach Bedarf durch zusätzliche Fachleute aus den Bereichen Gesundheit, Transport und Energie, Sozialverhalten und Medien, Wirtschaft und Finanzen, Staatsführung und Demokratie sowie den Polizei- und Sicherheitsdiensten. Auftrag der Beiratsmitglieder ist es darüber zu beraten, welche weitergefassten ethischen Auswirkungen die Art und Weise hat, auf die personenbezogene Daten erfasst und genutzt werden; die Beratungen sollen so transparent wie möglich sein.

4. Schlussfolgerung: Zeit zur Vertiefung der Diskussion

Privatsphären- und Datenschutz sind nicht das Problem, sondern Teil der Lösung. Zurzeit wird Technologie noch vom Menschen gesteuert. Es ist keine leichte Aufgabe, diese

potenziellen Entwicklungen als gut oder schlecht, wünschenswert oder schädlich, vorteilhaft oder nachteilig zu klassifizieren; noch schwieriger wird diese Aufgabe, wenn eine Reihe von potenziellen Tendenzen im Zusammenhang gesehen werden müssen. Entscheidungsträger, Technologieentwickler, Geschäftsentwickler und wir alle müssen uns ernste Gedanken darüber machen, ob und wie wir die Entwicklung von Technologie und ihre Anwendung beeinflussen wollen. Gleichermaßen von Bedeutung ist jedoch, dass die EU eine dringende Debatte über Ethos und darüber führt, wo in den Technologien der Zukunft die Menschenwürde ihren Platz hat.

Datenschutzgrundsätze sind nachweislich in der Lage, den Einzelnen und seine Privatsphäre vor den Risiken verantwortungsloser Datenverarbeitung zu schützen. Die sich heute abzeichnenden Tendenzen erfordern jedoch unter Umständen einen völlig neuartigen Ansatz. Deshalb starten wir eine neue Debatte darüber, inwieweit die Anwendung von Grundsätzen wie Treu und Glauben und Rechtmäßigkeit ausreicht. Die Datenschutzgemeinschaft kann unter Einsatz des bestehenden Instrumentariums, zu dem beispielsweise Vorabkontrollen und Genehmigungen gehören, eine neue Rolle übernehmen, weil keine anderen Einrichtungen dazu ausgerüstet sind, eine derartige Datenverarbeitung zu prüfen. Angesichts des rasanten Tempos der Technologie, globaler Innovation und der Angeschlossenheit des Menschen bietet sich uns eine Gelegenheit, Aufmerksamkeit zu erregen, Interesse zu wecken und Konsens aufzubauen.

Wir hoffen, mit dieser Stellungnahme einen Rahmen für eine breitere und tiefergehende Diskussion darüber bereitzustellen, wie die EU die Integrität ihrer Werte sicherstellen und gleichzeitig die Vorteile der neuen Technologien willkommen heißen kann.

Geschehen zu Brüssel am 11. September 2015

(**unterzeichnet**)

Giovanni BUTTARELLI
Europäischer Datenschutzbeauftragter

Anmerkungen

[1] Quelle: GSMA Intelligence.

[2] Das mooresche Gesetz, das besagt, dass sich die Zahl von Transistoren, die auf einem Mikrochip installiert werden können, ungefähr alle 18 Monate verdoppelt, gilt allgemein als erwiesen; Moore, Gordon E. (19.04.1965). „Cramming more components onto integrated circuits“, Electronics. 22.08.2011.

[3] Nathan Eagle, Alex (Sandy) Pentland, ‘Reality mining: sensing complex social systems’, Journal Personal and Ubiquitous Computing Band 10 Ausgabe 4. März 2006, S. 255–268. Shoshana Zuboff schreibt in „Big Other: surveillance capitalism and the prospects of an information civilization“, Journal of Information Technology (2015) 30, S. 75-89,: „Aufgrund der allgegenwärtigen Vermittlung durch den Computer wird fast jeder Aspekt der Welt in einer neuen symbolischen Dimension als Ereignisse, Objekte und Prozesse dargestellt; Menschen sind auf neue Art sichtbar, kennbar und als Gemeingut nutzbar.“ Nach Aussage von Zuboff wird eine „neue universale Architektur entstehen“, die sie „Big Other“ nennt - „eine allgegenwärtige Ordnung aus vernetzten Einrichtungen, die Alltagserfahrung - ob Toaster oder Körper, Mitteilen oder Denken - aufzeichnet, modifiziert und zur Handelsware macht, und alles im Zeichen der Einrichtung neuer Wege, um Geld und Profit zu machen“; S. 77, 81.

[4] „BBC Micro Bit computer's final design revealed“ 7.7.2015, http://www.bbc.com/news/technology-33409311(Zugriff 10.09.2015); „No assembler required: How to teach computer science in nursery school“, The Economist, 1.8.2015.

[5] Gemäß der PWC-Liste der zehn weltweit größten Unternehmen nach Marktkapitalisierung (am 31. März 2015 aktualisiert) hat keines der zehn nach Marktkapitalisierung größten Technologieunternehmen seinen Hauptsitz in der EU (acht sind US-Unternehmen, zwei stammen jeweils aus China und Taiwan).

[6] „Big Data bezieht sich auf das exponentielle Wachstum in der Verfügbarkeit und der automatischen Nutzung von Informationen; gigantische digitale Datensätze im Besitz von Unternehmen, Regierungen und anderen großen Organisationen, die anschließend mittels Computeralgorithmen intensiv analysiert werden (daher der Name; Analytik)“, Stellungnahme 03/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung. In einem Bericht des Weißen Hauses von 2014 werden Big Data als „Die zunehmende technologische Fähigkeit, eine zunehmende Menge von zunehmend unterschiedlichen Daten mit zunehmender Geschwindigkeit zu erfassen, zu aggregieren und zu verarbeiten“ beschrieben; siehe Big Data: Seizing Opportunities, Preserving Values, Executive Office des US-Präsidenten („Podesta-Bericht“), Mai 2014.

[7] Gemäß EU-Recht (Richtlinie 95/46/EG, Artikel 2 Buchstabe a) bezeichnet der Ausdruck „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“. Diese Definition stimmt im Großen und Ganzen mit der vom Europarat im Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (unter der Bezeichnung Übereinkommen 108 bekannt) und in den OECD-Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten getroffenen überein. Für eine tiefergehende Analyse siehe „Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ der Artikel-29-Datenschutzgruppe, WP136.

[8] Siehe beispielsweise den Vortrag der Vorsitzenden der US-Kartellbehörde aus dem Jahre 2014: "Die Ausbreitung von angeschlossenen Geräten, die ständig fallenden Kosten für das Erheben, Speichern und Verarbeiten von Informationen und die Fähigkeit von Datenmaklern und anderen, Daten offline

und online zu kombinieren, bedeutet, dass praktisch unbegrenzte Mengen an Verbraucherinformationen von Unternehmen angesammelt und auf unbegrenzte Zeit gespeichert werden können. Unter Einsatz prädiktiver Analysetechniken gelingt es ihnen, daraus überraschend viel über jeden einzelnen von uns zu erfahren;“ einleitende Bemerkungen von Edith Ramirez, FTC-Vorsitzende, „Big Data: A Tool for Inclusion or Exclusion?“, Washington, DC 15. September 2014. Sandy Pentland äußert sich dazu wie folgt: „Sozialphysik ist eine quantitative Sozialwissenschaft, die zuverlässige, mathematische Verbindungen zwischen Informations- und Ideenfluss einerseits und menschlichem Verhalten andererseits beschreibt … mit ihrer Hilfe sind wir in der Lage, Vorhersagen über die Produktivität von kleinen Gruppen, von Abteilungen in Unternehmen und sogar von ganzen Städten zu treffen.“ Dabei handelt es sich um „das, was für den Aufbau besserer sozialer Systeme“ (S. 4, 7) und „dafür erforderlich ist, dass (Beamte, Unternehmensmanager und Bürger) die Werkzeuge der Anreize sozialer Netzwerke dazu nutzen können, *neue Verhaltensnormen zu etablieren* (S. 189) (von uns kursiv gesetzt); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

[9] Eurobarometer Spezial Nr. 431 zum Datenschutz, Juni 2015, und Pew Research Panel-Umfrage (Januar 2014) über die Öffentliche Wahrnehmung von Datenschutz und Sicherheit nach Snowden. Ein durchschnittlicher Besuch einer einzigen Website führt, einer Studie zufolge, zu 56 Datenerhebungsvorgängen, so Julia Angwin *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). In dem Bericht des Weißen Hauses über Big Data aus dem Jahre 2014 heißt es: „beispiellose Rechnerleistung und -raffinesse … sorgen für ein Machtungleichgewicht zwischen den Dateninhabern und jenen, die die Daten absichtlich oder versehentlich liefern“; „bei einigen der größten Herausforderungen, die sich bei dieser Prüfung herausstellten, geht es darum, wie Big-Data-Analysetechniken eine derartig undurchsichtige Entscheidungsfindungsumgebung … erzeugen, dass sich die Autonomy des Einzelnen hoffnungslos in einem Algorithmen-Dschungel verstrickt.“

[10] Nach Angaben der Erhebung über öffentliche anonyme Daten von 1990 ist es wahrscheinlich, dass 87% US-Bürger anhand ihrer jeweiligen fünfstelligen Postleitzahl in Kombination mit Geschlecht und Geburtsdatum identifiziert werden können; siehe Paul Ohm ‘Broken promises of privacy: responding to the surprising failure of anonymisation’, UCLA Law Review 2010 und ‘Record linkage and privacy: issues in creating new federal research and statistical info’, April 2011. DNA ist einmalig (mit Ausnahme von eineiigen Zwillingen) und, solange die jeweilige Person am Leben ist, stabil. Sie enthält Informationen über Ethnie und Krankheitsveranlagung und kann zur Bestimmung anderer Familienmitglieder herangezogen werden. Im Januar 2013 gelang es Forschern, anhand von anonymen DNA-Daten aus öffentlich zugänglichen Ahnenforschungsdatenbanken Einzelpersonen und Familien zu bestimmen ; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321–324 (2013). Siehe auch „Genaue Angaben über den Aufenthaltsort von Taxifahrern in New York City aus schlecht anonymisierten Logbüchern“, 23.06.2014 http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (Zugriff 10.09.2015). Siehe auch Stellungnahme 04/2007 der Artikel-29-Datenschutzgruppe zum Begriff „personenbezogene Daten“; Stellungnahme 03/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung; Stellungnahme 06/2013 der Artikel-29-Datenschutzgruppe über offene Daten und Wiederverwendung von Informationen des öffentlichen Sektors und Stellungnahme 05/2014 der Artikel-29-Datenschutzgruppe über Anonymisierung.

[11] Quelle: Gartner.

[12] Siehe beispielsweise die Podiumsdiskussion „Welche Zukunft haben amtliche Statistiken im Zeitalter von Big Data?“ der Royal Statistical Society, London 19. Januar 2015; http://www.odi.org/events/4068-future-official-statistics-big-data-era (Zugriff 10.09.2015).

[13] Zehn Technologien, die unser Leben verändern könnten: mögliche Auswirkungen und politische Implikationen, Scientific Foresight Unit, Parlamentarischer Forschungsdienst der EU, Januar 2015.

[14] Das EU-Arbeitsprogramm 2016 - 2017, Horizon 2020, unterstützt diese Entwicklungen, einschließlich groß angelegter Pilotprojekte, die sich mit der Privatsphäre und ethischen Fragen beschäftigen.

[15] Das Geschäft mit Versicherungen wird als „das ureigene Geschäftsmodell für das Internet der Dinge“ beschrieben; „Vom Fitness Tracker bis zu Flugrobotern - wie das „Internet der Dinge“ die Versicherungsbranche transformiert“, Business Insider 11.6.2015. Der Begriff der Preisdiskriminierung im Wettbewerbsrecht, der aus Artikel 102 AEUV abgeleitet ist, nach dem die missbräuchliche Ausnutzung einer beherrschenden Stellung zur „unmittelbaren oder mittelbaren Erzwingung von unangemessenen Einkaufs- oder Verkaufspreisen oder sonstigen Geschäftsbedingungen“ verboten ist, ist stark umstritten, siehe beispielsweise Damien Gerardin und Nicolas Petit Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles (Juli 2005), Arbeitspapier Serien-Nr. 07/05 des Global Competition Law Centre. Zu Big Data und ihrem (gemäß den Autoren noch nicht verwirklichten) Potenzial zur Beschleunigung der persönlich zugeschnittenen Preisgestaltung siehe das Executive Office des Präsidenten der Vereinigten Staaten, Big Data and Differential Pricing, Februar 2015, sowie eine kürzlich durchgeführte Analyse, die zu dem Schluss kommt, dass für eine persönlich zugeschnittene Preisgestaltung üblicherweise die Verarbeitung von personenbezogenen Daten notwendig ist, bei der daher der Transparenzgrundsatz des Datenschutzrechts beachtet werden muss, nach dem Unternehmen die Betroffenen von dem Zweck der Verarbeitung ihrer personenbezogenen Daten informieren müssen: wenn Unternehmen ihre Preise individuell an den jeweiligen Kunden anpassen, dann müssen sie das offenlegen. Und wenn ein Unternehmen Cookies zur Bestimmung von Personen verwendet, dann muss das Unternehmen gemäß der Datenschutzrichtlinie für elektronische Kommunikation die jeweilige Person über den Zweck der Cookies informieren“; Arbeitsentwurf von Frederik Borgesius „Online Price Discrimination and Data Protection Law". Verfügbar unter folgender Adresse: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (Zugriff 10.09.2015).

[16] Medizinprodukte werden im EU-Recht gemäß der Richtlinie 93/42/EWG des Rates über Medizinprodukte, wie gemäß Richtlinie 2007/47/EG des Europäischen Parlaments und des Rates vom 5. September 2007 geändert, definiert. Bezüglich der Datenschutzimplikationen von „Mobile Health“, siehe EDSB-Stellungnahme 1/2015.

[17] Nach Eurostat nutzen 21% aller Einzelpersonen und 19% aller Unternehmen in der EU Cloud-Storage-Dienste.

[18] "Wenn das weltweite Internet ein Land wäre, dann wäre es der zwölftgrößte Stromverbraucher in der Welt, d. h. sein Verbrauch läge ungefähr zwischen dem von Spanien und von Italien. Das entspricht ungefähr 1,1 bis 1,5 Prozent des globalen Stromverbrauchs (in 2010) und den Treibhausgasen, die von 70 bis 90 großen (500 Megawatt) Kohlekraftwerken jährlich erzeugt werden.“ Natural Resources Defense Council, Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers 2014.

[19] Bericht der Studie „SMART 2013/0043 - Uptake of Cloud in Europe".

[20] Quelle: Eurostat.

[21] Der Begriff „Share Economy“ wurde als irreführend kritisiert: "The Sharing Economy Isn't About Sharing at All“, Giana M. Eckhardt und Fleura Bardhi, Harvard Business Review, 28.01.2015.

[22] Rachel Botsman und Roo Rogers, *What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

[23] Future of Privacy Forum, ‘User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy’, Juni 2015.

[24] Siehe Workshop der US-Kartellbehörde vom 9. Juni 2015 über „Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy“, https://www.ftc.gov/news-

events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (Zugriff 10.09.2015).

[25] Bezüglich der Datenschutzimplikationen von Flugrobotern oder pilotenferngesteuerten Luftfahrtsystemen siehe EDSB-Stellungnahme zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Ein neues Zeitalter der Luftfahrt — Öffnung des Luftverkehrsmarktes für eine sichere und nachhaltige zivile Nutzung pilotenferngesteuerter Luftfahrtsysteme", November 2014.

[26] Quelle: Boston Consulting Group.

[27] Gartner.

[28] DeepFace, der Gesichtserkennungsalgorithmus von Facebook, hat Berichten zufolge eine Erfolgsrate von 97% - besser als ein Mensch; DeepFace: Closing the Gap to Human-Level Performance in Face Verification, veröffentlicht in dem Bericht über die IEEE-Konferenz über Computer Vision und Mustererkennung, Juni 2014.

[29] Robo ist als eine „Maschine, die sich in der Welt befindet und fühlt, denkt und handelt" definiert worden; Bekey, G, Current trends in robotics: technology and ethics, in Robot Ethics - The ethical and social implications of robotics, The MIT Press2, 2012, S. 18. Schätzungen zufolge werden in den Jahren zwischen 2013 und 2016 22 Millionen Serviceroboter verkauft worden sein; IRF World Robotics Report, 2013. Bezüglich AI (künstliche Intelligenz) siehe Rise of the Machines, Economist, 09.5.15 und Pew Research Centre Internet Project 2014. Ein AI-Unternehmen bedingte sich bei seiner Übernahme durch ein führendes Technologieunternehmen 2014 die Einrichtung eines Ethik- und Sicherheitsrats sowie das Verbot des Einsatzes von AI für militärische oder sicherheitsdienstliche Zwecke aus; Forbes, Inside Google's Mysterious Ethics Board, 03.02.2014.

[30] Pentland, *Social physics*, S. 147

[31] Siehe Anmerkung 9 oben. Pentland *Social Physics* S.153: "Große Fortschritte in der Gesundheitsversorgung, im Transportwesen, in der Energiewirtschaft und in der Sicherheit sind durchaus möglich … was das Erreichen dieser Ziele verhindert, sind in der Hauptsache Besorgnisse hinsichtlich des Datenschutzes und die Tatsache, dass noch kein Konsens bezüglich der Kompromisse zwischen personenbezogenen und gesellschaftlichen Werten besteht." Die Debatte um die Ebola-Pandemie, die 2014 in Westafrika ausbrach, ist ein gutes Beispiel für diese falsche Dichotomie zwischen der Privatsphäre des Einzelnen und gesellschaftlichen Bedürfnissen. Der Verlauf und die Dauer von Krankheiten sind schon immer mittels Umfragen und Erhebungen verfolgt worden, die jedoch schnell veralten und von denen es sich nur schwer extrapolieren lässt, um Vorhersagen über den nächsten Ausbruch zu treffen. Es liegen einige Beispiele für die Verwendung von „Big Data" zur Verfolgung von Malaria-Epidemien in Namibia und Kenia sowie der Verfolgung der Wirksamkeit von behördlichen Warnhinweisen während der Schweinegrippe-Krise in Mexiko im Jahr 2009 vor. Zu Datenquellen gehören beispielsweise Mobiltelefonrufdaten, aus denen der den Ruf abfertigende Antennenstandort hervorgeht und die eine grobe Approximierung des Standorts des Anrufers und seines Bestimmungsorts in Echtzeit geben können. Das Sammeln dieser Daten ist nicht zielgerichtet - eine Unterscheidung zwischen jenen, die an Ebola erkrankt sind, und jenen, die nicht von Ebola betroffen sind, ist nicht möglich. Eine gemeinnützige Organisation aus Schweden kartografierte die Mobilität der Bevölkerung in Westafrika; die Daten wurden jedoch nicht genutzt, weil sich Mobiltelefongesellschaften weigerten, die Daten an autorisierte externe Forscher weiterzugeben; als Grund wurde angegeben, dass diesbezüglich behördliche Anweisungen vorliegen müssten; die Behörden wiederum führten Datenschutzerwägungen an, die gemäß EU-Recht nicht zu rechtfertigen wären; http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola. (Zugriff 10.09.2015).

[32] EDSB-Stellungnahme 3/2015

[33] Eine Big-Data-Annahme, dass „N=alle", bezieht sich darauf, dass alle Datenpunkte und nicht nur eine Stichprobe betrachtet werden, Viktor Mayer-Schönberger und Kenneth Cukier, *The Rise of Big*

Data: How it's changing the way we think about the world, 2013. Gemäß dem Argument des Lissabonner Rats und des Progressive Policy Institute wird Wohlstand dadurch vermehrt, indem die „digitale Dichte" - „die pro Kopf in einer Volkswirtschaft genutzte Datenmenge" - maximiert wird http://www.lisboncouncil.net/component/downloads/?id=1178 (Zugriff 10.09.2015). Die Internationale Arbeitsgruppe „Datenschutz in der Telekommunikation" (bekannt unter der Bezeichnung „Berlin Group") hat hinsichtlich der Datenschutzgrundsätze Ausnahmeregelungen für Big Data vorgeschlagen; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (Zugriff 10.09.2015). Das Weltwirtschaftsforum hat dazu aufgerufen, dass sich der Schwerpunkt von der Datenerhebung zu der Datennutzung verschieben und die Einwilligung zur Erhebung personenbezogener Daten nicht mehr länger erforderlich sein sollte; Unlocking the Value of Personal Data: From Collection to Usage, 2013.

[34] Siehe die vorläufige Stellungnahme des EDSB zu Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von Big Data.

[35] In Artikel 21 der Charta der Grundrechte heißt es: „Diskriminierungen, insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung, sind verboten." Viele dieser Datenkategorien („aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben")erhalten durch Artikel 8, Richtlinie 95/46/EG, vermehrten Schutz.

[36] Bezüglich des Konzepts eines digitalen öffentlichen Raums siehe Ambition numérique: Pour une politique française et européenne de la transition numérique, French Digital Council, Juni 2015 S. 276; Bruce Schneier plädiert für die Schaffung von „öffentlichen Räumen" im Internet, „die sich nicht in Privatbesitz befinden", wie öffentliche Parkanlagen, *Data and Goliath*, S. 188-189; Sandy Pentland plädiert für einen „öffentlichen Datenraum", *Social Physics*, S. 179. Bezüglich der Beurteilung der Sicherheit des Veröffentlichens von aggregierten Datensätzen als offene Daten, siehe Stellungnahme 06/2013 der Artikel-29-Datenschutzgruppe über offene Daten und Wiederverwendung von Informationen des öffentlichen Sektors.

[37] „Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent" http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. In Bezug auf qualifizierte Transparenz, siehe z. B. Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

[38] „Hinter der Technologie, die gesellschaftliche Beziehungen beeinflusst, stehen genau diese gesellschaftlichen Beziehungen", David Noble, 'Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools', in *Case Studies in the Labor Process*, Hrsg. Andrew Zimbalist, 1979. Siehe auch Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 S. 89-90; und Zuboff, 'Big Other' (zitiert in Anmerkung 3 oben).

[39] Siehe Stellungnahme 05/2014 zu Anonymisierungstechniken, angenommen am 10. April 2014 (WP 216).

[40] Hinsichtlich der eng ausgelegten Ausnahme von den Datenschutzregeln zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten, siehe Urteil des Gerichtshofs, Rechtssache C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů.*

[41] Der Begriff „Prosumer" wurde von Alvin Toffler in *The Third Wave*, 1980, geprägt. Bezüglich einer Diskussion der „Prosumer-Umgebung" und darüber, wie sie zu regeln ist, siehe Ian Brown und Chris Marsden, *Regulating Code*, 2013.

[42] Stellungnahme der Europäischen Gruppe für Ethik der Naturwissenschaften und der Neuen Technologien an die Europäische Kommission: Ethics of Security and Surveillance Technologies, Stellungnahme, Nr. 28, 20.05.2015, S. 74.

[43]Siehe beispielsweise Homer Economicus: The Simpsons and Economics, Hrsg. Joshua Hall, 2014.

[44] Das bedeutet, dass gemäß der konservativsten Definition von Fehler die Kreditauskünfte für 23 Millionen Amerikaner erhebliche Fehler aufweisen. Fünf Prozent der Kreditauskünfte über Studienteilnehmer wiesen Fehler auf, nach deren Korrektur sich ihre Bonität so verbesserte, dass sie billigere Darlehen beantragen konnten; US-Bundeshandelskommission, Bericht an den Kongress gemäß Paragraph 319 des Fair And Accurate Credit Transactions Act von 2003, Dezember 2012; Chris Jay Hoofnagle, How the Fair Credit Reporting Act Regulates Big Data (10. September 2013). Workshop über Big Data und Datenschutz, Future of Privacy Forum: Making Ends Meet, 2013. Abrufbar bei SSRN: http://ssrn.com/abstract=2432955.

[45] Gemäß dem WEF sind Daten eine wertvolle Ressource des Einzelnen; das Recht auf Besitz, Gebrauch und Verfügung dieser Daten kann Unternehmen und Behörden im Austausch für Dienstleistungen übergeben werden. Siehe kürzliche Vorträge u. a. von Andrus Ansip, dem Vizepräsidenten der Kommission, beispielsweise am 7.9.2015 beim Bruegel-Jahrestreffen mit dem Titel: 'Produktivität, Innovation und Digitalisierung - welche Herausforderungen für die globale Politik?': „Besitz und Verwaltung von Datenströmen, Verwendung und Wiederverwendung von Daten. Verwaltung und Speicherung von Daten. Sie sind das Fundament von wichtigen, im Entstehen begriffenen Sektoren wie Cloud Computing, das Internet der Dinge und Big Data."

[46] „Wem gehört also das Recht auf die Nutzung der Informationen und Daten, die nicht wirklich einem selbst gehören? Dies ist ein Thema, das über die Grenzen von Kommerz, Ethik und Moral hinausgeht und zu Fragen über die Privatsphäre und ihren Schutz führt"; Al-Khouri Nov. 2012, http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036. Siehe auch Margaret Jane Radin, Incomplete Commodification in the Computerized World, in The Commodification of Information 3, 17, Niva Elkin-Koren & Neil Weinstock Netanel Hrsg. 2002: „Es ist ein großer Unterschied, ob die Privatsphäre als ein Menschenrecht gilt, das jeder Mensch hat, gerade weil er ein Mensch ist, oder als ein Vermögensrecht, das in jemandes Besitz oder unter jemandes Kontrolle sein kann. Es besteht die allgemeine Annahme, dass Menschenrechte nicht auf dem Markt veräußerlich sind, während hinsichtlich Vermögensrechten die allgemeine Annahme besteht, dass sie auf dem Markt veräußerlich sind."

[47] Das von mehreren in der EU ansässigen Unternehmen unterstützte Crosscloud-Projekt des MIT Computer Science and Artificial Intelligence Lab zielt darauf ab, „1) die Entwicklung von Multi-Nutzer-Software („sozialer Software")zu vereinfachen, indem einzig und allein Front-End-Entwicklung eingesetzt wird und die Rechte und die Privatsphäre von Nutzern respektiert werden. Und 2) Nutzern die Freiheit zu gewähren, sich ungehindert zwischen Anwendungen, Hardware-Plattformen und sozialen Netzwerken unter Wahrung ihrer Daten und sozialen Verbindungen zu bewegen"; http://openpds.media.mit.edu/#architecture (Zugriff 10.09.2015)

[48] Siehe Erläuterung zu Artikel 1 der EU-Charta der Grundrechte.

[49] Martha Nussbaum, Objectification, in Philopsophy and Public Affairs 24, 4, 1995.

[50] Urteil vom 15. Dezember 1983, BVerfGE 65, 1-71, Volkszählung.

[51] Siehe Europäische Gruppe für Ethik der Naturwissenschaften und der Neuen Technologien, Stellungnahme zu Ethik und Überwachung, S. 75. Ein auf Anzeigen ansprechender Algorithmus, so geht aus einer Studie hervor, war diskriminierend, da im Vergleich zu Frauen, die Online-Jobbörsen besuchten, Suchläufe durchschnittlich Anzeigen für höher bezahlte Stellen für Männer ergaben; Carnegie Mellon University und das International Computer Science Institute. Hinsichtlich der Tendenz, digitale Hilfskräfte standardmäßig mit einer weiblichen Stimme zu versehen, siehe beispielsweise Judy Wajcman, Feminist theories of technology. Cambridge Journal of Economics, 34 (1). S. 143-152, 2010.

[52] Giorgio Agamben, *State of Exeption, 2005.*

[53] Neil Richards, Neil und Jonathan King, Big Data Ethics (19. Mai 2014), Wake Forest Law Review, 2014.

[54] BBC, Informationsüberwachungsorganisation untersucht „Veräußerung von Daten durch Wohltätigkeitsorganisationen", 1.9.2015.

[55] Siehe Schreiben vom Future of Life Institute. In der päpstlichen Enzyklika *Laudato Si* heißt es wie folgt: „Dazu kommen die Dynamiken der Medien und der digitalen Welt, die, wenn sie sich in eine Allgegenwart verwandeln, nicht die Entwicklung einer Fähigkeit zu weisem Leben, tiefgründigem Denken und großherziger Liebe begünstigen. Die großen Weisen der Vergangenheit würden in diesem Kontext Gefahr laufen, dass ihre Weisheit inmitten des zerstreuenden Lärms der Informationen erlischt. Das verlangt von uns eine Anstrengung, damit diese Medien sich in einer neuen kulturellen Entwicklung der Menschheit niederschlagen und nicht in einem Verfall ihres innersten Reichtums. Die wirkliche Weisheit, die aus der Reflexion, dem Dialog und der großherzigen Begegnung zwischen Personen hervorgeht, erlangt man nicht mit einer bloßen Anhäufung von Daten, die sättigend und benebelnd in einer Art geistiger Umweltverschmutzung endet. Zugleich besteht die Tendenz, die realen Beziehungen zu den anderen mit allen Herausforderungen, die sie beinhalten, durch eine Art von Kommunikation zu ersetzen, die per Internet vermittelt wird. Das erlaubt, die Beziehungen nach unserem Belieben auszuwählen oder zu eliminieren, und so pflegt sich eine neue Art künstlicher Gefühlsregungen zu bilden, die mehr mit Apparaturen und Bildschirmen zu tun haben, als mit den Menschen und der Natur. Die derzeitigen Medien gestatten, dass wir Kenntnisse und Gemütsbewegungen übermitteln und miteinander teilen. Trotzdem hindern sie uns manchmal auch, mit der Angst, mit dem Schaudern, mit der Freude des anderen und mit der Komplexität seiner persönlichen Erfahrung in direkten Kontakt zu kommen. Darum dürfte es nicht verwundern, dass sich gemeinsam mit dem überwältigenden Angebot dieser Produkte eine tiefe und wehmütige Unzufriedenheit in den zwischenmenschlichen Beziehungen oder eine schädliche Vereinsamung breitmacht."

[56] Siehe Maßnahme 4 der EDSB-Strategie 2015-2020, Entwicklung einer ethischen Dimension für den Datenschutz.