



Auftakt zur Veranstaltungsreihe Digitale Gesellschaft NRW.EU
am 26.10.2015 in der NRW-Landesvertretung, Brüssel

Digitaler Binnenmarkt – Perspektiven für den IT-Standort Europa „Datenschutz: Eine Chance für Europa“

Impuls von

Dr. Frauke Gerlach, Direktorin Grimme-Institut

Die Überschrift zu meinem Impuls drückt eine optimistische Grundhaltung aus, eine Haltung, die von Zuversicht getragen wird und das Vertrauen atmet, dass sich die Dinge zum Besseren entwickeln mögen. Lassen Sie mich die Überschrift „Datenschutz: Eine Chance für Europa“ zunächst mit Fragezeichen versehen.

1. Fragezeichen

Dieses Fragezeichen steht für mich für die Nutzerinnen und Nutzer des Netzes, die das Thema informationelle Selbstbestimmung und Datenschutz dem Konsum und der Bequemlichkeit preisgeben oder gar einen – aus meiner Sicht verqueren – „Post-Privacy-Ansatz“ verfolgen.

Denn, man hat ja nichts zu verbergen und vor allem: es bricht eine schöne neue Welt der Transparenz an. Jeder kann von jedem alles wissen, jede Intimität. Dies soll das Gesellschaftsmodell der Zukunft sein? Eine gruselige Vorstellung für mich.



Und: Konsumieren ist orgiastisch, nicht nur wenn man bei Zalando Schuhe kauft. Was interessiert es mich, dass ich danach Monate lang mit Werbung gestalkt werde?

Da könnte ich sofort kulturpessimistisch werden und wünschte ich mir mehr „Punk“ von den Konsumenten. Die Kulturkritik von Johnny Rotten fällt mir dazu ein. Sie wissen schon, der aus den 1970-ern von den Sex-Pistols. Er sang damals: „No future. Your future dream is a shopping scheme.“ Also es geht eben auch um die Verantwortung der Konsumenten, es sind bei weitem nicht nur die Politik und die digitale Wirtschaft gefragt.

2. Fragezeichen

Mein zweites Fragezeichen gründet sich auf die Haltung der Wirtschaft, die mit Big Data einen stark wachsenden Wirtschaftssektor – zu Recht – ausschöpfen will. Der Kunde bezahlt mit seinen Daten, wenn etwas umsonst ist, das sollte ihm klar sein.

Es gilt aber auch der verfassungsrechtliche Grundsatz, dass ohne Wissen der Betroffenen keine Daten erhoben werden dürfen. Doch selbst wenn ich bezahle oder mich nur informiere, werden meine Daten monetarisiert.

Letztlich geht es im Kontext des privaten Datenschutzes um Vertrauen und Selbstbestimmung. Die Entscheidung, ob die Daten weitergegeben und verarbeitet, also letztlich monetarisiert werden, sollte transparent und von der Einwilligung der Nutzerinnen und Nutzer abhängen.

Mir sind die globalen Schief lagen für die europäische Wirtschaft sehr bewusst. Diese abzubauen ist das Ziel der Strategie der Kommission für einen digitalen Binnenmarkt für Europa. Das ist ein Kraftakt.



Die Währung, die aber die Wirtschaft nicht verspielen sollte, ist das Vertrauen der Kunden, die heute vielleicht noch leichtfertig sind, aber morgen, wer weiß?

Zugleich kann man den Datenschutz im privaten Sektor nicht mehr sauber von staatlichen Zugriffen trennen. Alle Verbindungsdaten können abgegriffen werden. Dass es auch getan wird, wissen wir seit den Enthüllungen von Edward Snowden aus dem Jahr 2013. Diese offenbaren, dass europäische Daten in den USA potentiell den US-Geheimdiensten zur Verfügung stehen.

Ein höchst unerwünschter Nebeneffekt von Big Data für die Wirtschaft, die allein aufgrund dieser Situation ein hohes Interesse daran haben muss, dass Zugriffe der staatlichen Willkür entzogen werden. Auch dies sichert das Vertrauen der Kunden.

Nicht zuletzt geht es bei einem wirkungsvollen europäischen Datenschutz um das Ausspähen von Daten der Unternehmen, also um das verfassungsrechtlich geschützte unternehmerische Wirken, seien es Innovationen, Patente oder Strategien. Hierzu sollen auf europäischer Ebene Cybersicherheitsstrategien entwickelt werden, ein schwieriges Unterfangen, aber für die Entwicklung eines digitalen Binnenmarktes eine notwendige Maßnahme.

3. Fragezeichen

Mein drittes Fragezeichen: Kommen die Politik und die europäischen Institutionen ihrer Verantwortung nach?

Bei Verantwortung der Politik und dem Datenschutz im digitalen Zeitalter geht es um Verantwortung gegenüber den Bürgerinnen und Bürgern sowie der Wirtschaft.

Es geht aber auch um die grundrechtskonforme Begrenzung der staatlichen Überwachungsgelüste. Konnte man in der analogen Welt überwiegend die Nutzung der Daten im privaten Kontext noch fein säuberlich von staatlichen Eingriffen



trennen, so verschränken sich durch Big Data die Zugriffsmöglichkeiten sowohl von Geheimdiensten als auch für global agierende Unternehmen.

Das Netz ist Instrument der Freiheit und zugleich Instrument der Kontrolle.

Die Europäische Kommission hat sich zum Ziel gesetzt, die Freiheit **und** den Datenschutz zu sichern. In der Mitteilung der Kommission „Strategie für einen digitalen Binnenmarkt für Europa“ vom 6. Mai 2015 heißt es, ich zitiere:

„Wenn es um den Schutz personenbezogener Daten und die Wahrung der Privatsphäre geht, fühlt sich die EU höchsten Standards verpflichtet, wie sie durch die Artikel 7 und 8 der Grundrechtscharta garantiert werden.“

Ziel der Kommission ist es, mit der Datenschutz-Grundverordnung das Vertrauen in digitale Dienste zu verbessern und den Schutz der Personen im Hinblick auf die Datenverarbeitung durch alle Unternehmen, die ihre Dienste auf dem europäischen Markt anbieten, zu erhöhen.

Fast gleichzeitig mit der Mitteilung der Kommission hat die Regierung der Bundesrepublik Deutschland einen Entwurf zur Vorratsdatenspeicherung ins Parlament eingebracht, der nach der Bewertung der Bundesbeauftragten für den Datenschutz, Frau Voßhoff, gegen Artikel 7 und 8 der Grundrechtscharta verstößt.

Dabei beruft sie sich auch auf den Europäischen Gerichtshof, der die herausragende Bedeutung dieser Grundrechte wiederholt betont. Der Gesetzentwurf zur Vorratsdatenspeicherung wurde am 16. Oktober 2015 beschlossen. Er sieht die anlasslose Speicherung von Verbindungs- und Standortdaten von Telefon- und Internetnutzern vor. Die Inhalte der SMS können gelesen werden.

Die Pflicht zur Speicherung trifft die Telekommunikationsunternehmen, die die Daten ihrer Kunden bis zu zehn Wochen lang speichern müssen.



Damit können Persönlichkeits- und Bewegungsprofile der Bürgerinnen und Bürger anlasslos erstellt werden. Dies widerspricht der Rechtsprechung des Bundesverfassungsgerichts.

In seiner Entscheidung vom 2.3.2010 hat es bereits ein entsprechendes Gesetz zur Vorratsdatenspeicherung, das sich in den verfassungsrechtlichen Kernfragen nicht wesentlich von dem in diesem Monat verabschiedeten „Datenstaubsaugergesetz“ unterscheidet, nicht nur für verfassungswidrig, sondern für nichtig erklärt. Das Bundesverfassungsgericht führt in seiner Entscheidung aus, ich zitiere:

„Das die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss.“

Vieles spricht dafür, dass das höchste deutsche Gericht über die Regelungen zur Vorratsdatenspeicherung aus diesem Monat nicht anders urteilen wird als im März 2010.

Auch auf EU-Ebene wurde die einschlägige Regelung zur Vorratsdatenspeicherung gekippt. Dies ist gut ein Jahr her.

Am 8.4.2014 hat der Europäische Gerichtshof die Vorratsdatenspeicherrichtlinie der EU (2006/24/E) für ungültig erklärt, da sie nach Ansicht des Gerichts einen Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten beinhaltet.

Vor diesem Hintergrund sehe ich Europa als Chance, damit die Vorgaben der Gerichte zur Vorratsdatenspeicherung umgesetzt werden und nicht nur auf dem Papier stehen, sondern sich die Staatlichkeit sich auch daran hält, wir also von einer Verfassungswirklichkeit beim Datenschutz gegenüber dem Staat sprechen können.

Es gibt weitere gute Nachrichten für den Datenschutz aus Europa:



Optimistisch stimmen mich zwei weitere Entscheidungen des Europäischen Gerichtshofes. In seinem Urteil vom 6. Oktober hat der EuGH das „Safe Harbor“ Abkommen faktisch für unwirksam erklärt, indem es entschieden hat, dass der Transfer von personenbezogenen Daten in die USA nicht mehr auf der Grundlage dieser Vereinbarung erfolgen dürfen.

Die EU-Kommission hat das Abkommen im Jahr 2000 mit den USA geschlossen. Danach konnten sich US-Unternehmen verpflichten, den EU-Datenschutzstandards zu entsprechen, sie wurden dann zertifiziert und die personenbezogenen Daten auf diesem Schutzniveau übertragen. So die Vereinbarung und die Theorie.

Die Zertifikate wurden im Wesentlichen nicht überprüft und die Unternehmen hielten sich nicht daran.

Dieses Urteil könnte also für die europäische Datenwirtschaft wegweisend sein. Wenn sich der Rechtsrahmen an dem europäischen Standard orientiert, gäbe es in dieser Hinsicht geringere Wettbewerbsverzerrungen, als es gegenwärtig der Fall ist.

Außerdem bietet die Gerichtsentscheidung zu „Safe Harbor“ eine Grundlage dafür, dass sich Bürger gegen die Datenverwerter Google, Facebook, Amazon und wie sie heißen, rechtlich wehren können.

Das dritte wegweisende Urteil des EuGH ist aus Mai 2014 und implementiert das „Recht auf Vergessenwerden“. Suchmaschinenbetreiber wie Google müssen auf Antrag Informationen aus ihren Suchergebnissen streichen, wenn Informationen die Persönlichkeitsrechte betroffener Personen verletzen.

Bei der Ausgestaltung dieses Rechts kommt es darauf, ob es ein öffentliches Interesse an der Person gibt. Hier gilt es das Spannungsverhältnis zwischen



journalistischer Arbeit und Persönlichkeitsrechte aufzulösen, ein bekanntes Konfliktfeld.

Bei diesen Gedankengängen möchte ich es belassen und komme abschließend auf den Titel meines Impulses zurück: „Datenschutz eine Chance für Europa“.

Ich bin noch nicht beim Ausrufungszeichen, sehe aber in der Entwicklung des europäischen Datenschutzes nach der kurzen Reflexion meiner Fragezeichen durchaus Chancen:

Ich fange mit der Politik und den Europäischen Institutionen an:

1. Die Europäische Kommission hat in ihrer Mitteilung 6.5.15 ein sehr optimistisches Bild von der Stärkung des Datenschutzes und die gleichzeitige Verbesserung der Rahmenbedingungen für die digitale Wirtschaft und den europäischen Wirtschaftsraum gezeichnet.

Die Verknüpfung sehe ich tatsächlich als Chance, weil sie die Debatte befeuert und die Verwilderung des Netzes in Sachen Datenschutz in Arbeit nimmt. Die EU als digitalen Landschaftsgärtner kann ich mir gut vorstellen.

Mit dem Europäischen Parlament und dem Europäischen Gerichtshof gibt es zwei Institutionen, die sich für die Realisierung des Datenschutzes einsetzen. Damit gibt es zwei Ranger, um im Bild zu bleiben, die bei der Gestaltung eine zentrale Rolle spielen.

Und die Wirtschaft?

2. Bei der Wirtschaft geht es um die Vertrauensbeziehung zwischen Kunden und Unternehmen. Eine Kernfrage für den Kunden ist die der Ausgestaltung der Einwilligung in die Verwertung seiner Daten.



Der vom Zentralverband der Werbewirtschaft organisierte Prozess zur Entwicklung von Kodizes über die Verwendung nutzungsbasierter Online-Werbung ist sehr positiv; Trägerverbände sind u.a. der VPRT und der BDZV. Der Kunde trägt seinerseits ebenfalls Verantwortung und von ihm kann die Sorgfalt in eigenen Angelegenheiten erwartet werden. Hierzu benötigt er allerdings Informationen und Transparenz über die Art und Weise der Datenverwendung.

Optimistisch bin ich, weil ich den Eindruck habe, dass die Haltung der deutschen Wirtschaft zum Datenschutz eine grundsätzlich positive ist. Außerdem messe ich dem „Safe Harbor“-Urteil im Hinblick auf die Wettbewerbsverzerrungen durch die globalen Player wie Google und Amazon eine wesentliche Bedeutung zu.

Schlussendlich: Was ist mit uns Nutzerinnen und Nutzern?

3. Die aktuellen Ereignisse und Debatten offenbaren und vertiefen die Erkenntnisse um den Datenschutz im Internet. Dies wird, so hoffe ich, den freiheitlichen Grundsatz der Eigenverantwortung im Umgang den Daten stärken und das Bewusstsein für unsere Wertegemeinschaft schärfen.

Und zuletzt: Kinder sind ja unsere Hoffnung:

So kann ich mir sehr gut vorstellen, dass die nächste Netzgeneration mehr „Punk“ will und sieht, dass es auch andere orgiastische Erlebnisse als den Konsum gibt.