



Foto: istock/scanrail

"Wir müssen den Zugriff auf unsere Daten beschränken"

VERÖFFENTLICHT AM 08.04.2016

Grenzenlose Kommunikation, cloud computing, selbstfahrende Autos – technisch ist heute vieles möglich. Doch wir verstehen noch nicht, was das für unsere Gesellschaft wirklich bedeutet, sagt die Rechtswissenschaftlerin Indra Spiecker gen. Döhmann – und fordert mehr IT-Sicherheit. Ein Interview.



TEXT

CORINA NIEBUHR >

Aktuell entstehen mehrere neue Rechtsgrundlagen für die digitale Gesellschaft. Welchen Bereich halten Sie für besonders wichtig?

Die zunehmende Vernetzung und die zentrale Speicherung unserer Daten. Wir lagern Unmengen an Daten an einer Stelle zwischen – bei den Telekommunikationsanbietern, bei Cloud-Anbietern, bei IT-Dienstleistern aller Art –, was Zugriffsmöglichkeiten schafft, die beispiellos sind. Das müssen wir erst einmal richtig verstehen, was das für uns, unsere Gesellschaft, auch für unsere Wirtschaft bedeutet. Man kann aktuell in vielen Bereichen leider nicht von Grundlagen für die Entstehung von Rechten sprechen. Vielmehr erleben wir momentan einen massiven Eingriff in unsere Rechte und die Schaffung von Grundlagen dafür. Es ist für die meisten nur noch nicht spürbar, was das bedeutet, wenn Staat und Unternehmen den Schleier des Nichtwissens wegziehen und mit unseren Daten wirtschaften, uns steuern und überwachen.

Sie sprechen die Vorratsdatenspeicherung an ...

... die ein sehr gutes Beispiel für diese Problematik ist. Der Staat sichert sich mit der Vorratsdatenspeicherung Zugriff auf massive Datenbestände, die er dann mit anderen Datenbeständen verknüpfen kann. Algorithmen erlauben ausdifferenzierte Rasterungen dieser Daten. Wer solche Möglichkeiten schafft, baut eine Infrastruktur für Unrecht und weniger für Recht, weil diese Möglichkeiten unglaubliche Begehrlichkeiten und Missbrauchsgefahren auslösen – nicht nur beim Staat, sondern bei aller Art von Privatpersonen bis hin zu Kriminellen, all denen, die Zugriff auf diese Datenbestände haben oder ihn sich verschaffen. Ich halte das für gefährlich. Hinzu kommt, dass die Regelung zur Vorratsdatenspeicherung in vielerlei Hinsicht unklar und unbestimmt ist, die der Gesetzgeber gerade verabschiedet hat. Ein Beispiel ist, ob der Staat auch Zugriff auf Chaträume hat oder nicht. Auch die Verschlüsselungsdebatte, ob es Zwangsschnittstellen für staatliche Zugriffe in jedem Programm geben muss, zeigt, wieviel Unsicherheit über Rechte und deren Schutz besteht - und damit auch über Rechtsgrundlagen für Eingriffe. Die Auseinandersetzung in den USA um die Entschlüsselung des

IPhones ist da nur ein Aspekt der Gesamtproblematik.



ZUR PERSON



Indra Spiecker genannt Döhmann (Foto: Uwe Dettmar)

Indra Spiecker ist Professorin für Öffentliches Recht, Informations-, Umweltrecht und Verwaltungswissenschaften an der Goethe-Universität Frankfurt. Ihre Forschungsschwerpunkte liegen unter anderem im Informations-, Datenschutz und IT-Recht.

Anwälte, Ärzte, Journalisten – auch deren Daten werden gespeichert, obwohl sie die Informationen ihrer Mandanten, Patienten, Informanten schützen müssen.

Diesen Schutz der Berufsgeheimnisträger und ihrer Mandanten, so wie wir ihn kennen, gibt es mit der Vorratsdatenspeicherung nicht mehr. Der Staat darf auf die Daten zwar nicht zugreifen, sie müssen aber gleichwohl gespeichert werden. Wer es darauf abgesehen hat, kann einen Weg zu diesen Daten finden. Und das ist eine Gefährdung, die es vor der Vorratsdatenspeicherung in diesem Ausmaß nicht gab. Jetzt ist sie existent, vom Staat aktiv geschaffen.

Wie steht es um Firmengeheimnisse? Womit ich nicht Korruption oder Steuerhinterziehung meine, sondern das Wissen, mit dem Unternehmen wirtschaften.

Hier ist der Problembereich eher in anderen Aspekten zu sehen, nämlich in der allgegenwärtigen Vernetzung, darin, dass immer mehr Unternehmenswissen über das Internet kommuniziert wird und auch immer mehr kommuniziert werden muss. Wer darauf Zugriff hat, kann Unternehmensgeheimnisse erfahren und gewichtige Einblicke nehmen. Für Wissensgesellschaften ist dies höchst problematisch, weil es gerade der gut gehütete Wissensvorsprung ist, auf den Unternehmen ihre Produktivität, ihr Wirtschaften aufbauen – der Schutz dieses Wissens ist also extrem wichtig. Dafür gibt es aber im Moment kein funktionierendes Rechtsregime. Das Geheimnisschutzrecht für Unternehmen ist bislang ausgesprochen wenig ausgestaltet; für diesen Bereich wird auf EU-Ebene gerade erst eine erste Richtlinie erarbeitet. Also es ist momentan nur sehr begrenzt möglich, dass Unternehmen sich in diesem Bereich überhaupt auf eine klare Rechtsposition zurückziehen und deren Einhaltung auch einfordern können.



FORSCHUNGSGIPFEL 2016

Wie kann die Rechtsetzung derart unvorbereitet sein? Die Digitalisierung und all ihre Herausforderungen sind ja nicht über Nacht gekommen.

Die Ursachen dafür sind ganz mannigfaltig.

Hat die Politik die Entwicklungen verschlafen?

Das kann man leicht an folgendem Beispiel ablesen: 1995 haben wir auf europäischer Ebene eine Datenschutzrichtlinie bekommen, die im Kern seither unverändert geblieben ist. 1995 war an die Technik, die wir



(Foto: Stifterverband)

Das zentrale Thema auf dem Forschungsgipfel 2016 ist "Digitalisierung". Dabei spielen auch Aspekte wie gesellschaftliche und technologische Rahmenbedingungen eine Rolle. Der Forschungsgipfel bringt Führungspersönlichkeiten und Fachexperten aus Wirtschaft, Wissenschaft, Politik und Zivilgesellschaft zusammen, um gemeinsam Lösungen dafür zu entwickeln, wie die Digitalisierung für den Innovationsstandort Deutschland genutzt werden soll. Der Forschungsgipfel 2016 findet am 12. April 2016 in Berlin statt. Der Stifterverband wird die Veranstaltung per Livestream ins Web übertragen.

ALLES ZUM FORSCHUNGSGIPFEL 2016 2

jetzt haben, aber gar nicht zu denken - nehmen Sie nur Cloud Computing, Smartphones, selbstlernende Roboter. Erst jetzt gibt es überhaupt eine Neuregelung, die Datenschutz-Grundverordnung, die aber auch erst 2018 in Kraft treten wird – und zudem in vielen Regelungen sehr abstrakt bleibt und viele neuere Problembereiche ungeregelt lässt. Es ist offensichtlich, was für ein langer Zeitraum der Nicht-Anpassung des Rechts ins Land gegangen ist, in dem faktisch niemand die neuen Entwicklungen begleitet und reguliert hat, und in dem deshalb auch kaum Kontrolle stattfand und stattfinden konnte. Dieser leere Raum hat Politik und Rechtsprechung massiv eingeschränkt, die Entwicklungen, die sich in der digitalen Welt überschlagen, adäquat zu begleiten und anzuleiten. Diese Diskussion um die Rolle der Digitalisierung, ihre Folgen und Nebenwirkungen und ihre Bedeutung für Gesellschaft und Recht müssen wir erst noch führen - und damit sind wir spät dran.

Warum haben die Aufsichtsbehörden, die klassischen Regulierungsbehörden, nicht mehr Druck ausgeübt?

Sie hätten sicherlich mehr Einfluss nehmen können, wenn man es nicht versäumt hätte, diese Behörden besser mit Personal und anderen Ressourcen auszustatten – ihren wachsenden Aufgaben gemäß. Also fehlt auf dieser Seite schlichtweg teilweise die Kraft, überhaupt Einfluss zu nehmen. Wenn man berücksichtigt, dass der Hamburger Datenschutzbeauftragte mit 14 Mitarbeitern, Sekretärin eingerechnet, die deutsche Aufsicht über die großen Mediengiganten Facebook, Google usw. betreut, ist das ein Witz. Es geht ja nicht etwa ums Nein-Sagen. Was wir in den klassischen Aufsichtsbehörden gebraucht hätten und auch jetzt dringend brauchen, sind interdisziplinäre Teams, die die dynamischen Entwicklungen auf den Informationsmärkten konstruktiv und rechtssichernd begleiten können und selbst Vorschläge entwickeln, wie gute Rechtsanwendung und -gestaltung für Deutschland und für Europa aussehen könnte und sollte.

Die IT-Giganten erzählen uns gute Geschichten, was schön und faszinierend an den neuen Möglichkeiten ist; die unangenehmen Nebenwirkungen aber überlassen sie gerne der Politik und anderen.



INDRA SPIECKER GEN. DÖHMANN

Professorin für Öffentliches Recht, Informations-, Umweltrecht und Verwaltungswissenschaften an der Goethe-Universität Frankfurt

Indra
Spiecker
genannt
Döhmann
(Foto: Uwe

Aber sind rechtliche Alleingänge nicht sowieso eher Makulatur – gerade weil die großen US-Player den Informations- und Kommunikationstechnikmarkt (IKT) derart beherrschen?

Dieses Argument kommt immer wieder: Auf den IKT-Märkten könne Europa keine Regulierung durchsetzen, wenn das Silicon Valley etwas anderes vorlebe. Natürlich kommen die US-amerikanischen und auch asiatischen Unternehmen mit ihren ganz eigenen wirtschaftlichen und rechtlichen Vorstellungen auf den europäischen Markt – und tun dann so, als seien unser Informations- und Datenschutzrecht schwierig und falsch, weil beides für die Europäer selbst ein großes Problem darstelle. Das ist natürlich zwangsläufig so aus ihrer Sicht: Anderes Recht und andere Wirtschaftsvorstellungen sind dann mühsam und lästig. Aber jeder, der seine Produkte in einer anderen Rechtsordnung anbieten will, muss sich an die dort geltenden Gesetze halten! Und wenn man das durchsetzt, wird man erleben, dass auch europäische Unternehmen auf einmal eine Chance haben, weil auch in Europa gute IKT entwickelt wird.

Man möchte in erster Linie seine Geschäftskultur durchsetzen und die europäischen Märkte möglichst unkompliziert bespielen.

Natürlich, da ist ja auch zunächst nichts falsch dran. Auseinandersetzungen mit europäischen Produkt- und Sicherheitsvorstellungen haben wir in allen möglichen Marktfeldern, da werden sie meist nur viel selbstverständlicher akzeptiert, wie im Pharmabereich beispielsweise. Wer mit einem neuen Arzneimittel Märkte in Europa erschließen will, muss sich an europäische Regeln halten und tut es auch. Klar, wir sind bei Arzneimitteln nicht im Datenschutz unterwegs wie mit IKT, aber dafür mit ebenso wichtigen anderen Rechten konfrontiert. Und lassen wir uns nicht blenden: Die IT-Giganten erzählen uns gute Geschichten, was schön und faszinierend an den neuen Möglichkeiten ist; die unangenehmen Nebenwirkungen aber überlassen sie gerne der Politik und anderen. Wir Juristen sehen das vielleicht etwas klarer, nicht zuletzt weil wir viel über Haftung nachdenken, und vielleicht sollten wir gelegentlich noch viel lauter sagen: Halt, Vorsicht, das ist vielleicht nicht alles gut, und darüber müssen wir uns Gedanken machen, wer die Rechnung am Ende bezahlt, und wer die Gewinner und die Verlierer sind.

Auch bei Juristen hat das Thema Datenschutz lange eine eher randständige Existenz gefristet, könnte man sagen ...

... was sicher daran liegt, dass Juristen die Bedeutung von Informationen und Digitalisierung eben auch lange nicht erkannt haben, und weil sie sich oft nicht sonderlich mit Informationstechnik beschäftigt haben. Und ohne geht es natürlich nicht. Datenschutzrecht kann man im Grunde nur noch mit einer hohen technischen Kompetenz betreiben, weil man verstehen muss, auf welcher technischen Ebene Datenströme ablaufen, wo die Knackpunkte sind, wo die Technologie in welche sozialen und rechtlichen Konstrukte hineingerät. Im IKT-Bereich haben wir zudem das Problem, dass jeder die Technik nutzt und uns die Nutzung sehr schön einfach gemacht wird, aber nur wenige verstehen, was bei all den Informations- und Kommunikationsprozessen im Hintergrund genau passiert. Juristen sind da keine Ausnahme.

Die User nehmen ihre Macht nur noch viel zu wenig wahr.

66

INDRA SPIECKER GEN. DÖHMANN

Noch einmal kurz zurück zur Dynamik der Entwicklungen. Wie geht deutsche und europäische Rechtsetzung in Zeiten digitaler Umbrüche, die noch dazu stark von einer anderen Wirtschaftskultur eingefärbt sind?

Wir kommen an gewissen Schnellschüssen bei Gesetzen und Regulierung wohl nicht vorbei, weil wir nicht alles sofort bis ins letzte Detail durchdringen können, teils aber schnell handeln müssen. Wenn das selbstfahrende Auto technisch möglich ist, können wir die Entscheidung nicht verschieben, ob unsere Rechtsordnung erst einmal fahren lassen will oder nicht. Und da kann es passieren, dass wir die zukünftige Entwicklung falsch einschätzen, dass es zu schlimmen Unfällen kommt oder auch nicht. Da kann es sein,

dass wir Entwicklungen laufen lassen, ohne eine umfassende Analyse betrieben zu haben – oder auch vorschnell ausbremsen. Parallel – und das klingt jetzt widersprüchlich – muss die Antwort des Rechts gerade deshalb aber sein, eben weil wir mit prognostischen Elementen umgehen müssen: Vorsicht, wenn wir nicht genau wissen, was auf uns zukommt, dann wollen wir lieber diesen Prozess etwas verlangsamen, die Entwicklungen begleiten und dann erst vollständig entscheiden. Wenn man es genau nimmt, hat diese Vorgehensweise dem Technikregulierungsrecht auch jenseits der digitalen Welt schon immer inne gewohnt. Wie gut dieser Weg klappen kann, zeigt etwa die Regulierung im Gentechnikrecht.

Viele nutzen ihre IT-Technik und -dienste mit mulmigem Gefühl, weil sie einerseits damit kommunizieren wollen und sich andererseits den Sicherheitslücken und AGBs ausgeliefert fühlen.

Studien belegen, dass die meisten Menschen tatsächlich den Eindruck der Machtlosigkeit haben, nach dem Motto: Ob ich als Einzelner WhatsApp nutze oder nicht, was macht es für einen Unterschied, wenn es doch alle anderen sowieso tun? Das Beispiel zeigt die fatale Denkschleife, in der wir uns befinden: Es ist doch genau der Einzelne, der den Unterschied macht, nämlich dann, wenn mit ihm noch tausende andere derselben Meinung sind, wenn man sich organisiert mit seinen Interessen – die User nehmen ihre Macht nur noch viel zu wenig wahr. Bei den Unternehmen ist das anders, da haben die großen US-amerikanischen IT-Firmen nach den NSA-Enthüllungen sofort begriffen, dass sie sich in einer äußerst brenzligen Situation befinden – nicht etwa aus Angst vor den Geheimdiensten, die ihre Cloud-Systeme durchsuchen, sondern vor der Reaktion der User, die ihre Daten sicherer verwahrt sehen wollen und deshalb woanders hingehen könnten – und dies zum Teil ja auch gemacht haben: Europäische Cloud-Anbieter stehen hoch im Kurs, und US-amerikanische Anbieter haben ihrerseits gezielt nach Europa ausgelagert.

Was würden Sie gerne vorantreiben?

Den gesamten Bereich der IT-Sicherheit. Wir müssen dafür sorgen, dass der Zugriff auf Daten beschränkt wird, und dies dann auch wirklich eingehalten und kontrolliert wird. Wenn das Internet diese berühmte Rückgratfunktion für unsere Gesellschaft hat, und ich denke das ist so und wird eher noch zunehmen, dann muss sich das auch im Schutz der technischen Infrastruktur und der Inhalte wiederspiegeln. Dann muss IT-Sicherheit und der Schutz vor Angriffen viel wichtiger sein als gegenwärtig. Es gibt haarsträubende Beispiele, wo wir einen adäquaten Schutz noch nicht entwickeln und wo fehlende IT-Sicherheit massive Auswirkungen haben kann, wie die Ransomware-Angriffe auf Krankenhäuser gezeigt haben.

Das ist eine Virus-Software, die innerhalb von Sekunden Teile des angegriffenen Rechners verschlüsselt und damit für den Moment unbrauchbar macht. Für das Entschlüsseln erpressen die Angreifer dann in der Regel Geld.

Wenn ein tonnenschwerer OP-Roboter in einem solchen Moment gerade in einem Menschen operiert, kann man sich ausmalen, was das bedeuten kann. Solche Szenarien sind kein Science Fiction, weshalb wir weitaus mehr Kraft und Ressourcen in IT-Sicherheit investieren müssen als bislang. So ein Roboter muss sich im Notfall auch anders bewegen lassen – dafür brauchen wir neue Softwarelösungen und technische Notfallmechanismen. Und das natürlich nicht nur im Krankenhaus. Denn diese neuen Gefahren dringen in alle möglichen Bereiche unserer Gesellschaft und Wirtschaft ein- und werden dies auch tun, wenn alles immer weiter über das Internet miteinander vernetzt wird.

QUELLE: HTTPS://MERTON-MAGAZIN.DE/"WIR-MÜSSEN-DEN-ZUGRIFF-AUF-UNSERE-DATEN-BESCHRÄNKEN"