
PROTECTION
PRIVACY
SECURITY
DATA
I
Like
Daten
Schutz!

Impressum

Herausgegeben von der Delegation der Linken in der Konföderalen Fraktion der Vereinigten Europäischen Linken / Nordische Grüne Linke

Besonderer Dank gilt allen AutorInnen und MitstreiterInnen die uns bei der Erstellung dieses Datenschutzreaders unterstützt haben und allen an der Datenschutzkonferenz beteiligte Gästen und OrganisatorInnen. Weitere Informationen zur politischen Arbeit von und mit Dr. Cornelia Ernst sowie alle Texte zum Thema Datenschutz sind zudem auf unserer Homepage: www.cornelia-ernst.de zu finden.

Bilder: Dr. Armin Krause, Seite 57: James Halliday (Unterliegt der Creativ Commons Lizenz CC BY-SA 2.0 und darf bei Namensnennung unter den gleichen Bedingungen weitergegeben werden.)
Titelbild: istock.com
Redaktion: Lorenz Krämer, Anja Eichhorn und Jan-Robert Karas
Gestaltung: Reiko Kammer
Druck: Laserline
Auflage: 500 Exemplare

GUE/NGL
Vereinte Europäische Linke/Nordische Grüne Linke
Parlamentsfraktion · EUROPÄISCHES PARLAMENT

DIE LINKE.
IM EUROPAPARLAMENT

Inhalt

„I LIKE DATENSCHUTZ“
Fachkonferenz am 14. Juli 2012 in Leipzig

Vorwort

Der Skandal um die Geheimdokumente des amerikanischen Geheimdienstes National Security Agency (NSA) hat die Dimension aufgezeigt, um die es beim Umgang mit Daten mittlerweile gehen kann. Hemmungslose Ausspähung von Millionen Menschen, anlasslos und als Prinzip, knallharte Überwachung von Institutionen der EU, der UN und Wirtschaftsspionage im großen Stil. Dank eines beispiellosen Datenmissbrauchs wurde der Glauben an Recht und Gesetz ebenso wie an „befreundete" oder „weniger befreundete" Staaten erschüttert. Daten sind die Währung des 21. Jahrhunderts geworden, stabiler als Öl oder Gold und ständig wieder verwertbar. Fehlende Regeln und der Missbrauch datenschutzrechtlicher Grundprinzipien ermöglichen spielend eine Totalüberwachung rund um die Uhr. Wenn die NSA in trautem Bunde und mit Hilfe anderer Geheimdienste, wie dem BND, eine halbe Milliarde Kommunikationsvorgänge überwacht, sind wir längst im Reich von „Big Brother" gelandet und müssen die überfällige Frage nach Sinn und Zweck von Geheimdiensten stellen. Wer jetzt noch glaubt, ohne den gesetzlichen Schutz personenbezogener Daten auskommen zu können, ist naiv oder leistet vorsätzlichem Handeln Vorschub.

Persönliche Daten werden heute täglich in riesigen Mengen generiert und verarbeitet. Dazu trägt praktisch jeder bei. Wer heute seinen Einkauf mit EC-Karte bezahlt, etwas auf Facebook postet, eine E-Mail verschickt oder ein Buch im Internet kauft, erschafft damit neue Daten, die etwas über sie oder ihn aussagen und die ebenso unweigerlich in irgendeiner Datenbank landen. Das ist zunächst weder besonders auffällig noch problematisch. Ein Versandhandel kann eben nicht liefern ohne Adresse und wenn man alle Einkäufe mit der Karte bezahlt, ist klar, dass die Bank hinterher wissen könnte, wo man einkaufen war.

Das Ganze ist aber nur solange unproblematisch, wie sicher ist, dass die Daten nur für den ursprünglichen Zweck benutzt und nicht einfach weiterverkauft werden. Überhaupt sollten nur die Daten erhoben werden, die für den jeweiligen Zweck nötig sind. Der Versandhändler und die Bank könnten die Daten, die sie ohnehin haben, auswerten und Kundenprofile erstellen, die viel über die Interessen und Gewohnheiten der Kunden aussagen, diese noch mit einigen Zusatzfragen über Alter und Zusammensetzung des Haushalts ausbauen und gewinnbringend an große Werbefirmen verkaufen. Solange die Konsequenz nur ist, dass mehr (und persönlich zugeschnittene!) Werbung ins Haus flattert, mag das nur unangenehm sein. Wenn diese Daten kombiniert in die Hände von Polizei und Geheimdiensten gelangen, ist an sichtbaren Konsequenzen wieder alles möglich. Jahrelang kann alles ohne Probleme voran gehen, bis plötzliche überraschende Anschuldigungen kommen, die sich aus ziemlich privatem Wissen spei-

sen. Diese Beispiele sind nur grob und kratzen lediglich an der Masse der gegenwärtigen Datenverarbeitung. Die hat sich seit den 70er Jahren stetig ausgeweitet und findet heute praktisch überall Anwendung. In den Personalsystemen von Firmen, bei Amazon, Facebook, bei der Krankenversicherung und der Bank, genauso wie bei den staatlichen Behörden. Hinzu kommt die wachsende Anzahl an Firmen, die im Auftrag anderer Unternehmen oder Behörden Daten sammeln und verarbeiten und dann die Ergebnisse zurück liefern. Wäre es erlaubt, die Daten und die daraus gewonnenen Erkenntnisse frei weiterzugeben, wären in kürzester Zeit unzählige Informationen über jeden von uns im Umlauf. Damit wäre auch der größte Teil an Vertraulichkeit im Alltag hin.

Aus diesem Grund haben sich seit den 70er Jahren in Deutschland, aber auch auf internationaler Ebene, Regeln zum Schutz der persönlichen Daten etabliert. In der EU wurde 1995 mit der Richtlinie 95/46/EG eine europaweit verbindliche Regelung zum Datenschutz getroffen. Die darin enthaltenen Grundsätze, Datenminimierung und Zweckbindung, sind bis heute die anerkannten Grundprinzipien des Datenschutzes. Durch die schnelle Weiterentwicklung des Internets seitdem, zeigen sich aber auch die Schwächen, da das Ausmaß der Datenverarbeitung von heute damals schlicht nicht abzusehen war. Hinzu kommt, dass der größte Teil der Datenverarbeitung in den USA und damit außerhalb der unmittelbaren Reichweite europäischer Gesetze stattfindet. Zugenommen hat insbesondere seit 2001 die Datenverarbeitung durch Behörden, die dazu durch die Verschärfungen der Antiterrorgesetze ermächtigt wurden. Dabei geht es weniger um die Kameraüberwachung von Straßen und Plätzen als vielmehr um die Daten von internationalen Überweisungen, Flugpassagierdaten sowie Telefon- und Internetverbindungen. Bei der Auswertung der Daten kommen Verfahren zum Einsatz, die unter dem Begriff profiling zusammengefasst werden und mit denen nach auffälligen Mustern in den riesigen Datensätzen gesucht wird, mit dem Ziel, „unbekannte Verdächtige“ zu finden. Obwohl es hier um äußerst sensible Daten geht, immerhin lassen sich daran Kommunikation und Reiseverhalten ablesen, ist oft unklar, wer alles Zugriff darauf hatte.

Daten kennen erst einmal keine Grenzen und lassen sich problemlos an viele Orte auf der Welt übertragen. Ein effektiver Datenschutz muss daher auf nationaler wie auf internationaler Ebene ansetzen. Die Richtlinie von 1995 legt Standards und Mindestanforderungen der Datenverarbeitung fest, muss aber von jedem einzelnen EU-Mitgliedstaat mit entsprechenden Gesetzen umgesetzt werden. Obwohl im Grunde die gleichen Bedingungen gelten, ergibt sich so in der EU dennoch ein Flickenteppich von 27, seit Juli 2013 sogar 28 verschiedenen Datenschutzgesetzen. Das gleiche gilt für die nationalen Aufsichtsbehörden und die Datenschutzbeauftragten. Manche der nun 28 sind

besser ausgestattet, andere schlechter. Sie sind aber in jedem Fall entscheidend wenn es darum geht, Verstöße aufzuspüren, festzustellen und zu ahnden. So ist eine Situation entstanden, die es Unternehmen erlaubt, das EU-Land mit den günstigsten Bedingungen hinsichtlich der Datenverarbeitung auszuwählen und so das höhere Schutzniveau in den anderen Ländern zu unterlaufen.

Eine umfassende Reform des europäischen Datenschutzes soll Abhilfe schaffen. Daher hat die Europäische Kommission im Januar 2012 zwei europäische Gesetze, eine Verordnung und eine Richtlinie, zur Modernisierung des Datenschutzes in der EU vorgeschlagen. Die Verordnung, die unmittelbar in allen EU-Ländern gelten wird und keiner eigenen Gesetze bedarf, soll an die Stelle der bewährten 95er Richtlinie treten. Aber auch die Verordnung wird nicht für den Bereich der Polizeiarbeit und Strafverfolgung gelten. Hierfür hat die Kommission eine Richtlinie vorgeschlagen, die dann wiederum der Umsetzung in allen Mitgliedstaaten bedarf. Erstmalig soll damit aber eine verbindliche Regelung geschaffen werden, die die polizeiliche Datenverarbeitung betrifft, unabhängig davon, ob Daten in das Ausland übertragen werden oder nicht. Damit blieb die Kommission hinter den Forderungen des Europäischen Parlaments zurück, dass im Sommer 2011 gefordert hatte, beide Bereiche in einem Instrument zusammenzufassen, um ein einheitliches Niveau in allen Fällen zu garantieren. Der Vorschlag für die Richtlinie für den Polizeibereich sieht nun leider ein schwächeres Schutzniveau vor als die Verordnung, geht aber dennoch über viele heute herrschende Standards in dem Bereich hinaus.

Insgesamt weisen die Vorschläge der Kommission trotz Nachbesserungsbedarf in die richtige Richtung. Die Arbeit im Parlament fängt damit allerdings erst an. Weil Datenschutz ein Querschnittsthema ist und eben fast alle Bereiche unseres Lebens und Wirtschaftens berührt, werden sich auch alle Interessenverbände betroffen fühlen und mit viel Geld und Aufwand versuchen, das Beste für sich herauszuholen. Das gilt insbesondere für amerikanische Firmen, die bei einem konsequenten Datenschutz, der auch durchgesetzt wird, um ihren Zugang zu den europäischen Märkten fürchten. Diesen koordinierten Versuchen, den Datenschutz in Europa auszuhöhlen und zu durchlöchern, muss entschieden entgegen getreten werden. Dazu bedarf es vor allem Wissen über den Datenschutz und über aktuelle Datenverarbeitung. Ohne die gezielte Vernetzung mit ExpertInnen und PraktikerInnen auf dem Gebiet, ist dies nicht zu machen. Gleichzeitig dürfen die Interessen der Menschen vor Ort, deren Daten ja schließlich verarbeitet werden, auf keinen Fall außer Acht gelassen werden.

Die Vernetzung und das Gespräch mit den ExpertInnen, wie das Gespräch zwischen BürgerInnen, PraktikerInnen und Politik, war das Ziel der Konferenz zum Datenschutz,

die ich im Sommer 2012 in Leipzig veranstaltet habe. Nur so wird es möglich sein, am Ende des langwierigen parlamentarischen Prozesses einen wirklich modernisierten Datenschutz zu schaffen, der fit für das 21. Jahrhundert ist.

Diese Broschüre versammelt in schriftlicher Form die Redebeiträge, wie sie auf der Konferenz „I like Datenschutz" im Juli 2012 in Leipzig gehalten wurden. Die Konferenz wurde gemeinsam von der Fraktion der Vereinigten Europäischen Linken / Nordisch Grüne Linke im Europaparlament und der Fraktion der LINKEN im Sächsischen Landtag veranstaltet. Am Ende befindet sich eine Übersicht über ausgewählte Forderungen der GUE / NGL Fraktion im Europaparlament an die Datenschutzgrundverordnung, die wir als Änderungen im Europaparlament beantragt haben. Dem besseren Verständnis der teilweise recht technischen Beiträge ist ein Glossar beigefügt, in dem sich hoffentlich alle nicht gerade alltäglichen Begriffe, die verwendet werden, einfach und schnell nachschlagen lassen.

Wir bedanken uns bei allen MitstreiterInnen der Konferenz „I like Datenschutz" sowie bei allen FreundInnen des Datenschutzes, die uns bei unserer Arbeit im Europaparlament tatkräftig zur Seite standen und stehen. Insbesondere bedanken wir uns bei Karsten Neumann, dem ehemaligen Datenschutzbeauftragten von Mecklenburg-Vorpommern, sowie bei Jule Nagel, Stadträtin in Leipzig, für die hervorragende Arbeit bei der Organisation. Mit gemeinsamer Kraft kämpfen wir um höchste Standards im Datenschutz. Wünschen wir uns allen einen langen Atem!

Denn „we like Datenschutz"!

Dr. Cornelia Ernst (MdEP)
Mitglied im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres

Lorenz Krämer
Parlamentarischer Assistent
Büro: Dr. Cornelia Ernst

Datenschutz Modern? Datenschutz in Sicherheit? Datenschutz in Arbeit!

Cornelia Ernst

Es ist doch schön, dass in Leipzig, der Stadt, welche erstmals auf Sachsens öffentlichen Plätzen Videokameras flächendeckend einsetzte, auch die erste Datenschutzkonferenz der noch jungen LINKEN stattfindet. Natürlich wäre auch Dresden mit dem Beispiel der Funkzellenabfrage geeignet, aber zugegebenermaßen waren die Demonstrationen gegen ACTA in Leipzig sachsenweit am stärksten. Und bevor die im Vertrag von Lissabon verankerte Europäische Bürgerinitiative ihre bürokratischen Hürden nehmen konnte, hat die erste ohne bürokratische Hürden einfach stattgefunden. ACTA. ACTA ist weg!

Die digitale Bürgerrechtsbewegung der NetzwerkerInnen hat mit der Verhinderung von ACTA ihren ersten großen Erfolg gefeiert, den auch die Frankfurter Allgemeine nicht weg beißen konnte, indem sie schrieb, der *„digitale Mob“*, *„eine die Demokratie gefährdende Meute, vor der die Politik kusche“* habe sich durchgesetzt. Es gibt gegenwärtig wohl kaum ein zweites europäisches und internationales Beispiel, das so klar beweist, dass außerparlamentarischer und parlamentarischer Druck erfolgreich sein kann.

Viele EuropaparlamentarierInnen, nicht nur der Grünen und der Vereinigten Linken, der Liberalen und letztlich auch der Sozialisten/Sozialdemokraten, haben sich aktiv gegen ACTA aufgestellt und Mehrheiten erzwungen, die zum bisher größten politischen Sieg des Europäischen Parlamentes führten. Der Widerstand gegen ACTA symbolisiert nicht nur den Protest gegen die Absicht, nach Gusto des Anwenderlandes das Netz zu zensieren und zu filtern und damit die Informations- und Kommunikationsfreiheit im Netz aufzuheben, sondern auch gegen eine Politik der Hinterzimmer und der Geheimdiplomatie, welche die BürgerInnen zu Objekten degradiert und damit ihre informationelle Selbstbestimmung beschneidet. Dahinter verbirgt sich die Gefahr, unter dem fiebrigen Wahn vermeintlich notwendiger Überwachung und Steuerung, freie Kommunikation als Teil der Privatsphäre, gleichberechtigten Wissenserwerb, ungehinderte Vernetzung als unverzichtbarer Teil beruflicher und persönlicher Verwirklichung politischen Interessen unterzuordnen, ihren Zugang zu beschneiden und das grundrechtlich definierte Verhältnis von BürgerInnen und Staat umzukehren. Es geht um die Wahrung von substantiellen Grundrechten – das ist eine der großen Herausforderungen der Gegenwart.

Die andere Herausforderung ist der Umgang mit Daten, insbesondere personenbezogenen Daten. Die Milliarden Daten, die in kürzester Zeit verfügbar sind, sind längst zu einem unschätzbaren Kapital geworden. Diese Datenmenge bietet nie dagewesenes Wissen um Sachverhalte, aber auch Menschen. Und das ist verführerisch. Technisch ist es bekanntlich eine Leichtigkeit, Menschen heute komplett „gläsern" zu machen, ihr Verhalten, ihre Wünsche, ihr Denken, ihr Umfeld, Berufstätigkeit, Gesundheit, politische Ausrichtung, Kaufverhalten, sexuelle Vorlieben, Lifestyle, jedes Stäubchen der Privatheit aufzustöbern, zu ge- oder missbrauchen. George Orwells Vision als vollendeter Alptraum. Personenbezogenen Datenschutz als Grundrecht zu wahren, ist eine Herkulesaufgabe der Gegenwart. Wie stark der Druck auf dieses Grundrecht ist, zeigt sich auch im „Musterländle" des Datenschutzes, für das wir Deutschen uns sehr gern halten, zumindest oft. Schaut man in die letzten beiden Jahre, dann häufen sich die Meldungen: „Big Brother kommt als Computerwanze", Stichwort Bundestrojaner, pauschale Überwachung von Handykontakten, die Speicherung von sensiblen Gesundheitsdaten, der Regelungswunsch nach einer Vorratsdatenspeicherung und das Meldegesetz, an dem niemand schuld sein will.

Datenschutz in der EU

Einerseits war es der Druck aus Mitgliedsstaaten wie u.a. Deutschland, Österreich, Niederlande, der beförderte, dass die EU 1995 mit ihrer Richtlinie 95/46 EG Mindeststandards für den Datenschutz der Mitgliedsstaaten festlegte, die zwar noch nicht für die justizielle und polizeiliche Zusammenarbeit galten, aber dafür sorgten, dass Datenschutz überhaupt ein Thema in der EU wurde. Andererseits wurde in den letzten Jahren immer mehr der Schutz personenbezogener Daten gegen das auf europäischer Ebene, im Unterschied zum deutschen Grundgesetz, verankerte Recht auf Sicherheit abgewogen. Dafür steht zum Beispiel die EU-Richtlinie zur Vorratsdatenspeicherung von 2006, die übrigens zurzeit vor dem EuGH verhandelt wird. Insbesondere durch sie wurde die ungestüme Sammelwut von personenbezogenen Daten auf europäischer Ebene multipliziert. Mit dem Stockholmer EU-Programm 2009 wurde politisch das Tor für eine neue Sicherheitsarchitektur aufgestoßen, die auf Kosten von BürgerInnen- und Freiheitsrechten konstituiert werden soll. Das zeigt zum Beispiel das SWIFT-Abkommen zwischen der EU und den USA, das sämtliche Bankdaten europäischer Bankkunden betreffend Swift-Überweisungen in das nichteuropäische Ausland wegen Terrorverdacht checkt, täglich 15 Mio Banktransaktionen von 8300 Banken.

Ebenso das Fluggastdatenabkommen der EU mit Australien oder den USA, welches Fluggesellschaften verpflichtet, Flugpassagierdaten von allen Reisenden, die die EU-

Grenzen überqueren, zum Beispiel an die *Black Box* Heimatschutzbehörde zu übermitteln. Diese Daten umfassen 34 Abfragen, sie sollen viele Jahre gespeichert werden. Betroffenenrechte gehören in die Rubrik Spaß. Ein besonders nachhaltiges Beispiel ist INDECT - Intelligentes Informationssystem zur Unterstützung von Überwachung, Suche und Erfassung für die Sicherheit von BürgerInnen in städtischer Umgebung. Das ist ein Projekt im Rahmen des 7. EU-Forschungsprogramms, das alle Überwachungstechnologien zu einem universellen Überwachungsinstrument einer erkenntnisgestützten, proaktiven Polizeiarbeit bündeln soll. Die Polizei soll mit Hilfe von INDECT verdächtige bewegliche Objekte orten und verfolgen. Als verdächtig könnte damit bereits ein Rennen oder Flüchten auf öffentlichen Straßen bewertet werden. So könnten Menschen, die einmal durch ihr Verhalten auffallen, lückenlos überwacht und verfolgt werden. Am INDECT-Projekt arbeiten mehrere Universitäten sowie private Unternehmen aus verschiedenen EU-Ländern, auch aus Deutschland, wie die Bergische Universität Wuppertal.

Drei Forderungen an einen modernen Datenschutz

Fakt ist, es hat in letzter Zeit eine große Sensibilisierung der Menschen europaweit für Fragen des Datenschutzes gegeben, auch in Ländern, die bislang nicht von sich hören ließen, wie Polen oder Tschechien. Die Erwartung an den neuen Datenschutzrahmen ist groß, weil all diese Fragen zutiefst das Leben der Menschen beeinflussen. Erwartet wird erstens eine deutliche Verstärkung der Schutzregeln bei personenbezogenen Daten. Sie muss beinhalten: einen *code of conduct*, Datensparsamkeit und -Vermeidung, Erforderlichkeit, Zweckbindung, Verhältnismäßigkeit, Transparenz und wirksamer Rechtsschutz der Betroffenen, Prinzip der Nichtdiskriminierung, unabhängige Kontrolle der Einhaltung des Datenschutzes sowie des angemessenen Schutzniveaus außerhalb der EU. Zweitens: Der Rahmen muss ein europäischer sein! Wir brauchen einen vereinheitlichten Datenschutz in der EU und darüber hinaus mit starken Schutzregeln und Betroffenenrechten.

Drittens müssen wir um höchste Standards kämpfen! Trotz der 95er Richtlinie gibt es noch immer große Unterschiede in der EU. Wie lange bleiben meine Daten aufbewahrt und wer kann da ran, wenn ich in Tschechien mit der EC-Karte an der Tankstelle bezahle? Darf meine belgische Telefongesellschaft mein Geburtsdatum verlangen? Klare Regelungen sind notwendig und am besten löst sich das mit einer für alle Mitgliedsstaaten verbindlichen Verordnung.

Das Datenschutzpaket

Seit Januar 2012 liegen seitens der Kommission Entwürfe für eine Datenschutz-Grundverordnung und eine Richtlinie zum personenbezogenen Datenschutz im Bereich Strafverfolgung und -vollstreckung auf dem Tisch. Ich möchte, da insbesondere der erste Entwurf von Herrn Klabunde aus dem Büro des Europäischen Datenschutzbeauftragten problematisiert wird, lediglich auf drei Aspekte eingehen:

Verordnung und Richtlinie. Das ist eine heiße Debatte mit unterschiedlichen Angriffszielen. In der deutschen Datenschutzwelt wird vielfach die Sorge ausgesprochen, dass mit einer Verordnung, die dazu führt, dass für deren Auslegung nicht mehr das BVG, sondern der EuGH zuständig ist, grundrechtsrelevante Nachteile zu Lasten des Rechtsschutzes entstehen können. Vor allem dann, wenn die Verordnung unter den erreichten Standards in Deutschland bliebe. Das BVG hat in den letzten Jahrzehnten durch seine Rechtsauslegungen erheblichen Anteil an der Weiterentwicklung des praktischen Datenschutzes in der Bundesrepublik aufzuweisen. So sehr das nachvollziehbar ist, so wenig kommen wir damit weiter. Die Frage ist eben nicht mehr, ob wir die europäische Harmonisierung vorantreiben, sondern wie. Damit schaffen wir europaweit mehr Rechtssicherheit, Vereinfachung und Klarheit für die Betroffenen. Ziel muss der höchste Standard sein, wir brauchen deshalb für die kommenden Verhandlungen die besten Vorschläge, Erfahrungen und Impulse, ganz besonders aus Deutschland. Auch diese Verordnung hat Spielräume für die Mitgliedsstaaten, zahlreiche Vorschläge in der Verordnung, etwa im Kapitel II Grundsätze, machen das deutlich.

Die bisherige Richtlinie von 1995 reicht für die Zukunft nicht aus. Viele der vorgeschlagenen Regelungen stellen schon jetzt einen Fortschritt dar, anderes ist zwingend nachzubessern. Neben dieser Debatte gibt es aber noch eine andere. Zahlreiche Mitgliedsstaaten, auch die Bundesrepublik, wollen für den Bereich Justiz und Inneres noch nicht einmal eine Richtlinie, sondern den bisherigen Rahmenbeschluss behalten. Es wird extrem schwierig, überhaupt eine Neuregelung auf diesem Gebiet zu erwirken, obwohl der Handlungsbedarf hier am größten ist. Wir sollten hart darum kämpfen, dass die Bundesrepublik einen Richtlinienentwurf unterstützt, der viel mehr Rechtssicherheit für betroffene BürgerInnen herstellen könnte. Und das sage ich obwohl der Richtlinienentwurf kein großer Wurf ist, aber er wäre zumindest ein Anfang.

Fortschritte – aber nicht genug

Wo sehen wir Fortschritte, was ist zu verbessern? Die Verordnung soll sowohl für den privaten, als auch den öffentlichen Bereich verbindlich gelten und auch für die Übermittlung von Daten in Drittländer oder an internationale Organisationen soll es Regelungen geben. Das ist gut so. Wir kritisieren aber, dass relevante Bereiche ausgespart wurden, wie die Organe der EU und wir vermissen substantielle Regelungen zum großen Thema Arbeitnehmerdatenschutz.

Es gibt einen Zuwachs an Rechten für die BürgerInnen, wie die ausdrückliche Einwilligung, Recht auf Vergessen, Berücksichtigung von Kindern und Jugendlichen, Recht auf Datenportabilität, Transparenz und Informationspflicht gegenüber den betroffenen Personen sowie Widerspruchsrechte. Aber das Widerspruchsrecht ist mir viel zu schwammig formuliert. Ähnliches betrifft die Definition von *profiling* bei der Verarbeitung von Daten. Der Abschnitt über Beschränkungen, die die Union oder die Mitgliedsstaaten bei den Betroffenenrechten vornehmen kann, darf so nicht bleiben, weil schlechthin „öffentliche Sicherheit" oder „sonstige öffentliche Interessen" keine hinreichenden Argumente für Beschränkungen sind.

Und nun zum Thema Datenschutzbeauftragte und Aufsichtsbehörden. Es ist gut, wenn deren Kompetenzen und Unabhängigkeit gestärkt werden, aber auch dies sollte in Bezug auf die Kommission zutreffen. Positiv ist auch, dass der Europäische Datenschutzausschuss verbindliche Kompetenzen erhalten wird. Wir sollten uns vergegenwärtigen, dass dieses Verordnungspaket für die Bundesrepublik vielleicht keinen riesigen Schritt bedeutet, für Europa ist es aber ein Quantensprung. Oder, wenn ich den ehemaligen Datenschutzbeauftragten von Mecklenburg-Vorpommern, Karsten Neumann, zitieren darf: „… die Mondlandung ist gelungen – auf dem Weg zurück zur Erde sollten alle auf riskante Flug- und Bremsmanöver verzichten".

Zum Verfahren

Der Schutz personenbezogener Daten ist keine elitäre Nebenaufgabe, sondern betrifft als Grundrecht einfach alle, jede und jeden. Die gegenwärtigen Gesetzesvorschläge sind das bedeutendste europäische Vorhaben zur Grundrechtsausgestaltung seit den 90er Jahren. Um nicht mehr und nicht weniger geht es. Deshalb bin ich froh, dass wir als LINKE eine Themenbreite debattieren, die die europäische, nationalstaatliche und regionale Ebene miteinander verbinden. Wir werden uns drei großen Fragen stellen: Datenschutz Modern? Datenschutz in Sicherheit? Datenschutz in Arbeit!

Das Datenschutzpaket aus Sicht des Europäischen Datenschutzbeauftragten

Achim Klabunde

Ich bedanke mich für die Einladung, hier aus der Sicht des Europäischen Datenschutzbeauftragten ein paar Worte zu den Vorschlägen der Kommission zu sagen. Ich sollte vielleicht vorausschicken, dass ich zum Zeitpunkt der Verabschiedung der Kommissionsvorschläge selbst noch im entsprechenden Referat der Kommission gearbeitet habe und zwischenzeitlich gewechselt habe. Das bringt mich als Person ein wenig in eine Zwischenlage zwischen den ursprünglichen Gedanken der Kommission und der sehr profunden und inhaltlich von mir voll unterstützten Auffassung des Europäischen Datenschutzbeauftragten.

Die Stellungnahme des Europäischen Datenschutzbeauftragten zum Datenschutzpaket ist dankenswerterweise auch bei den Materialien, die auf der Webseite der Veranstaltung zur Verfügung gestellt wurden, in der deutschen Fassung abrufbar, so dass Sie also alles nachlesen können.[1] Es ist eine sehr umfangreiche Stellungnahme, die 75 Seiten umfasst und sehr tiefgehend fast alle Aspekte der beiden vorgeschlagenen Instrumente durchleuchtet. Sie bietet damit auch sehr viel Material für die weitergehende Diskussion, auch im politischen Bereich.

Eine kurze Übersicht über meinen Vortrag. Ich denke Sie verzeihen mir, wenn ich kurz den Europäischen Datenschutzbeauftragten vorstelle, der ja auf der nationalen Ebene noch nicht so wahnsinnig sichtbar ist und dann grundsätzlich etwas dazu sage, warum es überhaupt Datenschutz auf übernationaler Ebene gibt und warum dies eine Notwendigkeit ist und es in diesem Rahmen ebenso notwendig ist, auf EU-Ebene etwas dazu zu unternehmen. Dann werde ich auf die Vorschläge der Kommission kurz eingehen und einige Sachfragen in diesem Zusammenhang etwas tiefer ausführen.

1 Zu finden unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf

Aufsicht, Beratung, Zusammenarbeit – der EDPS

Der Europäische Datenschutzbeauftragte (EDPS) existiert seit 2004. Damals wurde Peter Hustinx als Europäischer Datenschutzbeauftragter gewählt. Es gibt noch einen stellvertretenden Datenschutzbeauftragten, der ebenfalls von Rat und Parlament bestimmt wird. Die Amtszeit beträgt 5 Jahre, das heißt, wir sind in der zweiten Amtsperiode des Europäischen Datenschutzbeauftragten. Peter Hustinx wurde 2009 wiedergewählt und der stellvertretende Datenschutzbeauftragte Giovanni Buttarelli ist seit 2009 im Amt. Peter Hustinx war vorher niederländischer Datenschutzbeauftragter, auch mehrfach Vorsitzender der Artikel 29 Gruppe und Giovanni Buttarelli war vorher unter anderem Generalsekretär des italienischen Datenschutzbeauftragten. Der Sitz des EDPS ist in Brüssel, mitten zwischen Kommission, Parlament und Rat. Es arbeiten dort zurzeit etwa 50 Mitarbeiter.

Die Rechtsgrundlage ist die Verordnung (EG) 45/2001, ich denke man muss diese Verordnung auch im Rahmen der aktuellen Diskussion erwähnen, weil es ja nicht so ist, dass es im Moment keine Datenschutzregeln für die europäischen Institutionen gibt. Die Verordnung (EG) 45/2001 hat damals die Bestimmungen der Richtlinie von 1995 und auch der Telekommunikations- oder seinerzeit noch ISDN-Datenschutzrichtlinie aus dem Jahre 1997, in Recht für die Institutionen der damals noch Europäischen Gemeinschaften umgewandelt. Dass es dort trotzdem, wie Frau Ernst richtig gesagt hat, Handlungsbedarf gibt, im Rahmen der Reform auch die Regeln für EU-Institutionen anzufassen, wird von dem Europäischen Datenschutzbeauftragten ausdrücklich unterstützt. Durch die Änderung der Verträge im Rahmen des Vertrags von Lissabon ist mit der Einführung des Artikels 16, der das Recht auf Datenschutz im Vertrag verankert, die Stellung des Datenschutzes gestärkt worden. Zugleich ist auch in der Grundrechtecharta der EU, in den Artikeln 7 und 8, das Recht auf Datenschutz und das Recht auf Privatleben verankert. Damit ist der Datenschutz in den Verträgen, im Primärrecht der Union vorgesehen und auch dessen unabhängige Überwachung als Teil des europäischen Datenschutzrechts.

Der EDPS hat drei Aufgabenbereiche, die als Aufsicht, Beratung und Zusammenarbeit gekennzeichnet werden. Sie können das auch auf der Webseite des EDPS finden. Die Aufsicht ist natürlich die Kernfunktion eines jeden Datenschutzbeauftragten. Hier geht es darum, die Verarbeitung personenbezogener Daten durch alle Organe, Behörden, Institutionen der Europäischen Union zu überwachen. Das ist die Hauptaufgabe und eine der zwei aufwändigsten. Im Rahmen der Aufsicht werden auch Beschwerden von Bürgern bearbeitet, deren Daten durch die Institutionen verarbeitet werden. Man kann sagen, dass ein sehr großer Teil der Beschwerden sich auf Datenverarbeitung im

Arbeitsverhältnis bezieht, das heißt, der EDPS hat de facto einen großen Schwerpunkt seiner Tätigkeit im Bereich des Arbeitnehmerdatenschutzes. Außer Beschwerden führt der Datenschutzbeauftragte auch eigenständige Prüfungen durch. Wir besuchen dann die verschiedenen Institutionen und schauen uns die Datenverarbeitungssysteme direkt an. Der Aufsichtsbereich des EDPS erstreckt sich nicht in allen Fällen auf die Systeme der ehemaligen dritten Säule, also der Polizei- und Justizzusammenarbeit. Dort gibt es in vielen Instrumenten eigenständige Regelungen, die eigenständige Gremien einrichten. Der EDPS nimmt nur an einigen davon teil.

Das zweite wichtige Aufgabengebiet des EDPS ist die Beratung. Hier geht es insbesondere um die Beratung des europäischen Gesetzgebers. Der EDPS nimmt regelmäßig zu allen Gesetzgebungsvorhaben mit Datenschutzrelevanz Stellung. Wenn sie es uns denn erlaubt, beraten wir die Kommission schon bevor sie ihren Vorschlag verabschiedet und wir beraten dann auch den Rat und das Parlament mit öffentlichen Stellungnahmen, sobald der Kommissionsvorschlag auf dem Tisch liegt. Das betrifft nicht nur solche Großvorhaben, wie die Datenschutzgrundverordnung und die Datenschutzrichtlinie, die im Rahmen der Reform vorgelegt wurden, sondern auch alle Instrumente im Bereich der Polizei- und Sicherheitszusammenarbeit oder auch andere Vorhaben. Im Mai hat der EDPS zum Beispiel eine sehr kritische Stellungnahme zum ACTA-Abkommen vorgelegt, die auch im Innenausschuss des Europäischen Parlaments vertreten und seinerzeit von der Kommission sehr scharf angegriffen wurde. Man kann allgemein sagen, dass sich das Europäische Parlament dankenswerterweise bemüht, die Ratschläge des EDPS ernsthaft in Erwägung zu ziehen, sodass man da auch einen Erfolg dieser Maßnahmen sieht.

Der dritte Teil unserer Aufgaben, ich habe das bereits angedeutet, ist der Bereich Kooperation. Natürlich kooperieren wir auch mit den Institutionen die wir überwachen, indem wir Ratschläge geben und darauf hinweisen, wie Datenschutzbestimmungen in der Praxis umgesetzt werden können. Insbesondere aber geht es hier um die Kooperation mit den nationalen Datenschutzbehörden der Mitgliedstaaten in der „Arbeitsgruppe zum Schutz von Individuen bezüglich der Verarbeitung personenbezogener Daten“, die errichtet wurde durch Artikel 29 der bestehenden Datenschutzrichtlinie. Daher wird die Arbeitsgruppe Artikel 29 Gruppe genannt. Diese Arbeitsgruppe nimmt auch Stellung zu europäischen Gesetzesvorhaben und politisch wichtigen Vorgängen im Bereich des Datenschutzes in der EU. An dieser Arbeit nimmt der EDPS teil. Der EDPS ist auch Teil der Überwachungsgremien derjenigen speziellen Systeme der EU, in denen es eigene Rechtsgrundlagen gibt, also EURODAC, das Fingerabdrucksystem für Asylbewerber, SIS, das Schengen-Informationssystem und VIS, das Visa-Informationssystem. Systeme also, die bestimmte Aspekte der Freizügigkeit durch Überwachungsmaßnah-

men abdecken. Bei all diesen Systemen hat der EDPS, gemeinsam mit den nationalen Datenschutzbeauftragten, den Behörden für IT-Sicherheit und mit der Unterstützung von Experten für IT-Sicherheit, Inspektionen der Systeme durchgeführt und dazu Berichte verabschiedet. Darin wurde auch die Kommission aufgefordert, entsprechend Missstände abzustellen.

Eine Nebenbemerkung: die Kommission hat ja vor einiger Zeit vorgeschlagen, den Betrieb all dieser Systeme aus dem Aufgabenbereich der Kommission auszulagern und hat dafür eine eigene Agentur vorgeschlagen, die inzwischen von Rat und Parlament beschlossen wurde. Die Agentur wird in Estland errichtet, die Systeme werden in Frankreich und Österreich betrieben. Es scheint so zu sein, dass die Behebung von Missständen eine wenig zwischen der Kommission und der noch nicht so richtig existierenden Agentur hängt. Das ist auch ein Thema, wo eine gewisse Beobachtung sinnvoll ist, um zu verhindern, dass einige Dinge einfach vom Tisch fallen in dieser Übergangsperiode. So viel zu Funktion und Aufgabenbereich des EDPS.

Warum Datenschutz auf internationaler Ebene notwendig ist

Ich kann mich durchaus noch an die ersten politischen Diskussionen in Deutschland zum Thema Datenschutz erinnern, auch wenn das 38 Jahre her ist, als das erste deutsche Datenschutzgesetz erlassen worden ist, 1974 in Hessen und 1978 im Bund. Schon damals war die Frage der internationalen Beziehungen im Bereich der Verarbeitung personenbezogener Daten ein Thema. Schon in der Begründung des Bundesdatenschutzgesetzes von 1978 gab es Bestimmungen, die den Export personenbezogener Daten in das Ausland beschränkt haben. Die Erkenntnis damals war die, dass nichts so einfach ins Ausland verlagert werden kann wie Daten. Schon in den 70er Jahren war es möglich, durch elektronische Datenübertragungsmittel das Rechenzentrum eines Großunternehmens außerhalb der deutschen Grenzen aufzubauen. Es wäre auch möglich gewesen, die Verarbeitung der personenbezogenen Daten aus dem Geltungsbereich der deutschen Gesetze hinaus zu verlagern. Deshalb haben Deutschland und alle Länder, die zu dieser Zeit Datenschutzgesetze erlassen haben, eben als Schutz gegen diese Verlagerung eine Sperre für die Übertragung von personenbezogenen Daten ins Ausland eingebaut.

Das war der Ansatz zum Schutz personenbezogener Daten, der sich aber mit der Entwicklung als problematisch erwiesen hat, weil eben die Wirtschaft und die Unternehmenswirklichkeit nicht so gestaltet ist, dass wir rein nationale datenverarbeitende

Stellen hätten. Eine vollständige Trennung nach nationalen Gebieten war nicht sachgerecht und hätte sich als Hindernis in der wirtschaftlichen Entwicklung dargestellt. Deswegen wurde schon in den 80er Jahren auf internationaler Ebene begonnen nachzudenken, wie verhindert werden kann, dass Datenschutz zu Hemmnissen für Handel und Wirtschaftswachstum wird. Die internationale Diskussion hat in zwei Institutionen begonnen, die nicht in allen Fällen bindende Regeln erlassen können. Das eine ist die OECD, wo die entwickelten Industrieländer beteiligt sind. Die OECD hat 1980 Richtlinien für den Schutz personenbezogener Daten erlassen, die beinhalten, dass ein gewisser Mindeststandard festgelegt wird und wenn dieser Standard erreicht ist, sollten die Mitglieder der OECD auch die Übertragung zwischen ihren verschiedenen Ländern nicht blockieren. Ein ähnlicher Ansatz ist im Übereinkommen 108 des Europarates, das aus derselben Zeit stammt, festgelegt, wobei das Übereinkommen bereits die Grundsätze des Datenschutzes, wie wir sie heute kennen, beinhaltet. Es wurde noch durch ein Zusatzprotokoll ergänzt, dass die unabhängige Überwachung des Datenschutzes festschreibt, die im eigentlichen Übereinkommen noch nicht enthalten war. Mit diesen beiden haben wir im Prinzip eine vollständige Darlegung der Prinzipien des Datenschutzes.

Wie wir alle wissen, hat dann 1995 die Europäische Gemeinschaft eine bindende Richtlinie verfasst, die ein gemeinsames Datenschutzniveau für die gesamte EG festgelegte und damit die Voraussetzung geschaffen hat, innerhalb der EG und heute der EU, den grenzüberschreitenden Transfer von personenbezogenen Daten zu ermöglichen. Alle internationalen Instrumente, die hier erwähnt sind, sind heute zur gleichen Zeit in Überarbeitung. Alle Instrumente beruhen auf den Grundsätzen, wie sie in den 70er und 80er Jahren festgelegt worden sind. Überall besteht das Gefühl, dass das beim gegenwärtigen Stand der Entwicklung nicht mehr hinreichend ist.

Ein kurzer Überblick über den EU-Rechtsrahmen

Wir haben die eben erwähnte Richtlinie 95/46/EG von 1995 und den Rahmenbeschluss von 2008, der die Verarbeitung personenbezogener Daten im Bereich der Polizei- und Justizzusammenarbeit betrifft. Dann existieren noch einige weitere Instrumente. Die Verordnung (EG) 45/2001, die die Rechtsgrundlage für den Datenschutz im Bereich der EU-Institutionen ist und auch die Rechtsgrundlage für den EDPS darstellt. Weiter die Richtlinie 2002/58/EG, die Richtlinie über Datenschutz in der Telekommunikation, die im Rahmen der Telekommunikationsreform 2009 reformiert wurde, die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung, die aber auch im Bereich des Datenschutzrechtes gesehen werden muss, weil sie Ausnahmen zur 2002/58/EG

schafft. Dann gibt es die speziellen Rechtsgrundlagen der Systeme VIS, SIS und EURODAC sowie den Beschluss zur Errichtung von Eurojust, der Beschluss zur Errichtung von Europol, und schließlich die Prüm-Entscheidung. Letztere ist ein Ratsbeschluss zum Datenschutz, ebenfalls im Polizei- und Justizbereich.

Was macht nun die Reform der Kommission?

Sie führt die Datenschutzgrundverordnung ein, die die Richtlinie 95/46/EG ersetzen soll und führt die Richtlinie für den Datenschutz im Bereich der polizeilichen und justiziellen Strafverfolgung ein, die den Rahmenbeschluss von 2008 ersetzen soll. Alle anderen Instrumente werden von der Reform nicht berührt. Das ist einer der Kritikpunkte, den Frau Ernst schon angesprochen hat und den der EDPS angesprochen hat. Eigentlich verlangt der Lissabon-Vertrag, dass eine wirkliche umfassende Regelung für den Datenschutz geschaffen wird. Das würde bedeuten, dass alle Regelungsfelder berührt werden.

Nun gibt es verschiedene Möglichkeiten, das zu tun. Man kann alles auf einmal machen, was natürlich eine riesige Arbeit ist, wie ich aus eigener Erfahrung sagen kann, wenn man alle Vorbereitungen berücksichtigt, die getan werden müssen, um einen Vorschlag auf den Tisch zu legen. Oder man kann das in verschiedenen Stufen machen, dann wäre es aber sinnvoll, wenn man eine Planung vorlegt. Der EDPS hat in seiner Stellungnahme kritisiert, dass die Kommission nicht nur keinen umfassenden Reformvorschlag vorgelegt hat, sondern auch, dass sie keinerlei Planung vorgelegt hat, wann die weiteren notwendigen Schritte des Datenschutzes angepackt werden sollen. Hier besteht also großer Handlungsbedarf und wird vermutlich auch weiterbestehen, da nicht zu erwarten ist, dass von der Kommission schnell etwas zu dem Thema kommt.

Ich habe angedeutet, dass die Reform des Datenschutzes international diskutiert wird. Dazu muss man sagen, dass praktisch alle Sprecher, die sich in den letzten Jahren dazu geäußert haben, sagen, dass die Prinzipien des Datenschutzrechts, wie sie vor jetzt 17 Jahren verabschiedet worden sind, den Test der Zeit bestanden haben und die Prinzipien selbst sich als gültig erwiesen haben, die praktische Umsetzung jedoch mehr und mehr auf Probleme stößt. Die Ziele der Reform sind insbesondere die materielle Verbesserung des Schutzes und die Vereinheitlichung. Hier haben wir ein großes Problem in der EU insofern, als dass die bestehende Richtlinie erheblichen Spielraum lässt und es daher erhebliche Abweichungen in der Anwendung des Datenschutzes gibt. Die Gründe für die Notwendigkeit mit einer Reform einzugreifen, sind u.a. die technologische Entwicklung.

Wenn man heutiges Datenschutzrecht auf heutige Datenverarbeitungsbedingungen anwendet, bin ich immer überrascht, in wie vielen Fällen es eigentlich möglich ist, klar zu sagen, was das Datenschutzrecht verlangt. Auch wenn heute Datenverarbeitungsprozesse stattfinden, die sich in den 70er Jahren niemand vorstellen konnte. Aber die Weitsicht der Erfinder des Datenschutzes in den 70er und 80er Jahren, einen technologieneutralen Ansatz zu wählen, die Prinzipien festzulegen und nur ganz wenig konkrete Verfahren zu bestimmen, hat sich eindeutig als funktionstüchtig erwiesen. Das ist ein Prinzip, welches man in der jetzigen Reform anwenden sollte.

Offene Fragen im internationalen Datenverkehr

Ein Punkt aus europäischer Sicht zur Notwendigkeit der Reform ist, dass es aber eben doch Verhältnisse gibt, in denen Rechtsunsicherheiten auftreten. Ich will nicht sagen, dass alle Probleme angefasst worden sind. Aber eine der Fragestellungen ist zum Beispiel, wie man damit umgeht, wenn man Daten verarbeitet, die zwar auf eine Person beziehbar sind, die verarbeitende Stelle zum Zeitpunkt der Verarbeitung den Personenbezug aber nicht wirklich hat. Das ist zum Beispiel der Fall, wenn man von Internetbenutzern IP-Adressen sammelt oder auch nur Autokennzeichen, ohne dass man selbst diese Daten mit identifizierenden Daten in Verbindung bringt, die es ermöglichen würden, den Betroffenen anzusprechen. Dann kann man die Datenschutzrechte des Betroffenen, den man nicht identifiziert hat, nicht berücksichtigen, was Auskunfts- und andere Rechte angeht. Da würde die Verordnung insofern Klarheit schaffen, indem die verarbeitende Stelle nicht verpflichtet werden soll, nur zu dem Zweck, datenschutzrechtliche Anforderungen zu erfüllen, mehr Daten zu erheben, als für den eigentlichen Zweck der Datenverarbeitung nötig ist. Das ist eine Klarstellung, bei der mehr Rechtssicherheit geschaffen wird.

Andere Themen betreffen die territoriale Anwendbarkeit des Datenschutzrechtes. Das ist ein sehr großes Problem. Unterliegen große amerikanische Unternehmen, die massenhaft Daten von Europäern verarbeiten, irgendeinem nationalen oder europäischen Recht? Da gibt es sehr unterschiedliche Auffassungen, je nachdem auf welcher Seite der Mauer man steht. Ein großes Thema aus europäischer Sicht ist die fehlende Harmonisierung. 27 Mitgliedstaaten haben 27 unterschiedliche Gesetze,[2] und obwohl die Richtlinie zur Vereinheitlichung diente, ist es doch zu sehr unterschiedlichen Auslegungen gekommen, sodass ähnlich wie im Steuerrecht wir hier die Gefahr haben, dass

2 Zu finden unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf

es zum sogenannten *forum shopping* kommt. Das heißt, dass sich Unternehmen dort mit ihrer Datenverarbeitung ansiedeln, wo sie die geringste Überwachung durch Datenschutzbehörden und den geringsten Schutz durch Datenschutzrecht erwarten. Es gibt bestimmte Mitgliedstaaten, die sehr attraktiv für große amerikanische Unternehmen sind, wobei man nicht so genau weiß, ob es dort das Steuerrecht oder das Datenschutzrecht ist, das letzten Endes den Ausschlag gibt. Hier besteht in jedem Fall Handlungsbedarf.

Ein weiterer Punkt ist die Einbeziehung des Polizei- und Justizbereichs, wie schon ausgeführt und die gesamte globale Dimension. Das ist die Frage, wie die Transfers von personenbezogenen Daten außerhalb des Bereichs, der durch das EU-Recht ein einheitliches Schutzniveau hat, gestaltet werden können. Auch dort versucht die Reform Ansätze zu geben.

Gute Ansätze

Die Reformvorschläge versuchen, die erfolgreichen und wirksamen Prinzipien fortzusetzen, aber im Lichte der bestehenden Herausforderungen für den Datenschutz in ihrer Anwendung zu verbessern. Solche Grundprinzipien wie Datensparsamkeit und „eingebauter Datenschutz", *data minimisation* und *privacy by design*, werden im Entwurf der Reform ausdrücklich mehr hervorgehoben als im bisherigen Recht. Grundsätzlich konnte man beide Prinzipien schon aus dem bestehenden Recht ableiten, aber sie werden jetzt ausdrücklich als Anforderungen an die verarbeitenden Stellen gestellt. Die Diskussion zum „eingebauten Datenschutz" geht sogar auf internationaler Ebene im politischen Bereich dahin, dass man sich fragt, ob man nicht von den Herstellern von Technologien, die jetzt noch nicht vom Datenschutzrecht erfasst sind, solange sie keine Daten verarbeiten, verlangt, dass der Datenschutz eingebaut wird. Wie das rechtlich zu gestalten wäre, ist aber eine Frage, auf die ich zumindest im Moment noch keine Antwort weiß. Gerade einige kanadische Datenschutzbehörden, aber auch der EDPS, beschäftigen sich ganz intensiv damit, wie man den eingebauten Datenschutz verbessern kann.

Für mich als Techniker ist das einleuchtend. Bevor ich selbst in die Datenschutzbehörden eingestiegen bin, habe ich mich immer gefragt, wie man ein System laufen lassen kann, welches technisch die Datenschutzregeln nicht sofort realisiert, das Zugriffsschutz nicht fest eingebaut hat. Dann haben Juristen mir manchmal geantwortet: „Das muss nicht sein. Es ist ja verboten, dadurch ist der Schutz gegeben." Es scheint, dass sich die Einsicht, dass man mit technischen Maßnahmen den Datenschutz noch effek-

tiver machen kann als durch juristische Maßnahmen, immer weiter verbreitet. Das kann ich voll begrüßen, auch wenn es uns Techniker zugleich mit mehr Aufgaben versieht wie auch mit größeren Schwierigkeiten.

Bei der Umsetzung machen die Vorschläge der Kommission einige sehr gute Ansätze, was die Unabhängigkeit und die Ausstattung der Datenschutzbehörden mit entsprechenden Ressourcen, Rechten und Befugnissen betrifft, auch bezüglich der Zusammenarbeit der Datenschutzbehörden für bessere Konsistenz in der praktischen Umsetzung. Dann bemüht sich die Kommission, auch einige Verwaltungsverfahren zu vereinfachen, indem zum Beispiel die Meldepflicht für Datenverarbeitung abgeschafft wird und hier mehr Eigenverantwortung eingeführt werden soll. Ein ganz umfangreiches Kapitel der Reform beschäftigt sich damit, die Entscheidungen der Datenschutzbehörden auf nationaler Ebene mehr zu vereinheitlichen. Sie schlägt hier ein Verfahren vor, dass insbesondere Unternehmen zugutekommt, die in mehr als einem Mitgliedstaat tätig sind. Diese Unternehmen sollen nur noch mit der Datenschutzbehörde an ihrem Hauptsitz zu tun haben, gleichzeitig sollen sich aber bei Entscheidungen, die in mehr als einem Mitgliedstaat Auswirkungen haben, alle betreffenden Datenschutzbehörden zusammensetzen und eine gemeinsam Linie für diesen Fall festlegen. Dafür gibt es das sogenannte *consistency* oder Kohärenzverfahren, in dem die gemeinsame Linie dann mit dem europäischen Datenschutzrat abgestimmt wird, der die Artikel 29 Gruppe ersetzt.

Muss es eine Verordnung sein?

Der EDPS unterstützt ausdrücklich den Ansatz der Kommission die Richtlinie durch eine Verordnung zu ersetzen, die direkt anwendbar und ist und im Gegensatz zu einer Richtlinie, nicht der Umsetzung durch die Mitgliedstaaten in nationales Recht bedarf, um wirksam zu werden. Nun ist es ein wenig übertrieben, das so über diese Verordnung zu sagen. Mir wurde erklärt, dass man so etwas eine „hinkende Verordnung" nennt. Es sieht aus wie eine Verordnung, verhält sich aber in einigen Teilen wie eine Richtlinie. Es sind viele Stellen enthalten, an denen steht: „Die Mitgliedstaaten stellen sicher, dass …", „Die Mitgliedstaaten legen fest …", „Die Mitgliedstaaten bestimmen …". Das heißt, diese Verordnung ist nicht zu 100% EU-Recht, das bis zur untersten Ebene durchschlägt, sondern diese Verordnung sieht in vielen Fällen Befugnisse für die Mitgliedstaaten vor, hier tatsächlich nationale Regelungen zu treffen. Ich denke das ist ein Punkt, den man in Deutschland besonders berücksichtigen muss, weil hier die Befürchtungen über die Subsidiarität eine große Rolle spielen. In der Tat ist diesen Befürchtungen im Instrument schon Rechnung getragen worden, zum Teil geht Kritik an der Verordnung auch dahin, dass sie nicht weit genug geht. Beim Thema des Arbeit-

nehmerdatenschutzes etwa legt die Verordnung es den Mitgliedstaaten in die Hand, genauere Regelungen zu treffen. Ich kann aus meiner Erfahrung sagen, dass gerade aufgrund von Argumenten aus Deutschland diese Bestimmung erwogen und aufgenommen worden ist.

Der EDPS hat die Verordnung im Großen und Ganzen begrüßt, mit Kritik in einigen Details. Zur Richtlinie hat er aber gesagt, dass er „ernsthaft enttäuscht" ist, weil die Richtlinie weit hinter dem zurück bleibt, was man hätte erwarten können, sollen und müssen. Auch wegen der Konstruktion, die Richtlinie als ein vollständig eigenständiges Instrument aufzustellen, das noch nicht einmal dieselben Definitionen verwendet wie die Verordnung. Das birgt die Gefahr, dass im Verlauf der Gesetzgebung selbst grundlegende Definitionen in der Richtlinie völlig anders ausfallen können als in der Verordnung. Das heißt, dass dann zum Beispiel „personenbezogene Daten" im Polizei- und Justizbereich auf einmal eine andere Bedeutung hat als in der Wirtschaft oder der allgemeinen Verwaltung.

Aber einige positive Punkte möchte ich noch hervorheben. Die Nutzerkontrolle ist im Verordnungsentwurf verbessert worden, mit dem Recht auf Korrektur und Löschung. Es gibt sehr viel Diskussion über das „Recht auf Vergessenwerden". Zunächst bedeutet das einfach, dass jemand etwas, das er oder sie selbst ins Netz gestellt hat, auch wieder zurückrufen kann, wenn es keinen Grund gibt, die Daten zu behalten. In der juristischen Formulierung ist das natürlich komplex und kann Nebeneffekte haben. Aber die Befürchtung, die von einigen Unternehmen, die von dieser Regelung betroffen würden, vorgetragen wird, dass damit die Orwell'sche Funktion eines Wahrheitsministeriums eingeführt würde, ist aus der bestehenden Formulierung wirklich nicht abzuleiten. Klarstellungen sind auch zu dem Thema „Einwilligung" vorgesehen, auch wenn das nur einer der Gründe für rechtmäßige Datenverarbeitung ist. Nicht-Aktivität sollte nicht als Einwilligung gedeutet werden. Das Widerspruchsrecht ist gestärkt, die Transparenzpflicht, das heißt die Informationspflichten, sind verbessert. Es ist ein Ansatz gegeben für ein Verbandsklagerecht, ebenfalls eine Neuerung. Neu eingeführt wird die *accountability*, womit stärker auf die Eigenverantwortung der verarbeitenden Stelle gesetzt wird, die dann auch nachweisen können muss, dass sie den Datenschutz erfolgreich umgesetzt hat. Im vorbeugenden Bereich werden Datenschutzfolgeabschätzungen eingeführt, die Unternehmen durchführen sollen, bevor sie eine neue Datenverarbeitung einführen. Neu eingeführt werden europaweit auch betriebliche Datenschutzbeauftragte und die umfassende Pflicht zur Meldung von Sicherheitsverletzungen, sogenannten *data breach notifications*. Das ist eine Regelung, die es insbesondere in den USA bereits gibt, die nun für alle datenverarbeitenden Stellen kommt. Die Unabhängigkeit der Datenschutzbeauftragten wird neu verankert. Der EuGH hatte ja in einem

Verfahren gegen Deutschland entschieden, dass einige Landesdatenschutzbeauftragte eben nicht hinreichend unabhängig waren, weil sie Teil der normalen Landesverwaltung waren. Zurzeit läuft auch ein Verfahren gegen Österreich, wo der nationale Datenschutzbeauftragte Teil des Bundeskanzleramtes ist.

Eine weitere Neuerung betrifft die territoriale Anwendbarkeit. Nach dem Vorschlag sind auch Datenverarbeitungen dem EU-Recht unterworfen, die sich an Bürger eines europäischen Mitgliedstaates richten, ganz unabhängig davon, wo sie stattfinden. Wenn also jemand in Russland mit einer Webseite Dienste für Menschen in Deutschland anbietet, wäre er auf jeden Fall nach dieser Vorstellung dem deutschen Recht unterworfen. Natürlich stellt sich da noch die Frage der Verfolgung, aber man ist einigermaßen optimistisch, weil es auch in anderen Rechtsbereichen wie z.B. dem Wettbewerbsrecht die Möglichkeit gibt, bestimmte Sanktionen zu vollstrecken und das unabhängig davon, ob das Unternehmen hier einen Sitz hat. Im Bereich der Datenübertragung ist der Versuch unternommen worden, die Regeln klarer zu gestalten, sodass sie sowohl wirksam als auch praktikabel sind. Ich hoffe damit habe ich die breite des Spektrums für die weitere Diskussion aufgezeigt

Prof. Lothar Bisky (MdEP), Dr. Cornelia Ernst (MdEP)

Datenschutz modern!

Joe McNamee

Zuerst eine kurze Einleitung zu *European Digital Rights*. EDRi ist eine Dachorganisation von 32 Bürgerrechtsorganisationen aus 20 europäischen Ländern, die sich für die Rechte und Freiheiten europäischer Bürger einsetzen. Unser Büro in Brüssel hat drei Mitarbeiter und wir beschäftigen uns mit Datenschutz, Vorratsdatenspeicherung, Urheberrecht und privatisierter Rechtsdurchsetzung im Internet. Im Großen und Ganzen also mit allen Vorschlägen, die einen Einfluss auf unsere digitalen Bürgerrechte haben können. Wir sind also was die FAZ „Internetfetischisten" nennt. Ich persönlich empfinde dies nicht als Beleidigung, da man diesen Begriff nur benutzen kann, wenn man keine Ahnung davon hat, was das Internet eigentlich ist.

Wie Datenschutz in Deutschland aussieht, wird in Brüssel bestimmt. Die Datenschutzbestimmungen werden durch Aufsichtsbehörden in den deutschen Ländern und auf Bundesniveau durch den Bundesbeauftragten für Datenschutz und Informationsfreiheit implementiert. Zurzeit haben wir eine europäische Richtlinie von 1995 und einen Beschluss über Datenschutz im Bereich der Sicherheit. Im Januar hat die Kommission eine Verordnung vorgeschlagen, um den Datenschutz europaweit zu harmonisieren.

Es erscheint vielleicht erstaunlich, dass eine Richtlinie von 1995 erst jetzt erneuert und modernisiert wurde. Dafür gibt es zwei Gründe. Erstens ist der Inhalt sehr kontrovers und frühere Kommissare waren nicht so streitlustig wie Kommissarin Reding. Aber es gibt auch einen zweiten sehr wichtigen Grund – die Prinzipien in der jetzigen Richtlinie gelten weiterhin und müssen uns erhalten bleiben. Es geht also nicht darum, die Prinzipien zu ändern, sondern sie „nur" anzupassen und existierende Probleme und Lücken zu identifizieren und zu beseitigen. Dies ist aber ein viel komplizierteres Problem als man denkt. Ich werde den nachfolgenden Beitrag in zehn Kapitel fassen – um relativ kurz eine Einleitung zu den neuen – und hoffentlich modernen – Elementen zu geben.

Hintergrund

Die Richtlinie zu modernisieren ist leider viel leichter gesagt als getan. Am Anfang schien alles ziemlich einfach. Kommissarin Reding hatte im September 2010 ein hochkarätiges Treffen für Industrie und Zivilgesellschaft organisiert. Dort hat die europäi-

sche Industrie erklärt, dass sie bereit sei, mehr Verpflichtungen zu übernehmen, wenn Datenschutz europaweit harmonisiert wäre. Von dieser Haltung ist nur noch sehr wenig übrig. Die Industrie beklagt sich mittlerweile kräftig über die neue Verordnung und sogar über die Verpflichtungen, die sie schon vorher hatte. Innovative und einfallsreiche Industrien behaupten, dass sie nicht in der Lage seien, zum Beispiel Lösungen für Datenportabilität zu finden. Notwendigkeit bleibt die Mutter aller Erfindungen, aber Datenschutz ist wohl ein wirksames Verhütungsmittel.

Und dann kommt die Haltung der Vereinigten Staaten dazu, was die Lage noch komplizierter macht. Im November hat jemand in der Kommission einen internen Entwurf der Verordnung *geleakt*. Zu dem Zeitpunkt waren sich die meisten Dienste der Kommission noch über den Vorschlag einig. Dann aber starteten die USA einen regelrechten Lobbyanfall gegen den Vorschlag. Das amerikanische Handelsministerium hat eine Analyse der Handelsaufsicht FTC verbreitet und hat dann die Generaldirektoren in der Kommission angerufen. Dies hat dazu geführt, dass fünf verschiedene Generaldirektionen der Kommission plötzlich Einwände gegen den Entwurf hatten. Die federführende Generaldirektion Justiz musste daher viele Aspekte der Verordnung abschwächen.

Ein wichtiger Teil des Vorschlags, nämlich der damalige Artikel 42, wurde nicht nur geschwächt sondern sogar gelöscht. Dieser Artikel war eigentlich dazu gedacht, das Problem von *PATRIOT Act* und *FISA Act* zu lösen. Diese beiden amerikanischen Gesetze geben den amerikanischen Behörden Zugang zu europäische Daten. FISA gibt den Amerikanern Recht auf Zugang zu Daten, wenn eine europäische Firma in den USA vertreten ist. Dies umfasst Zugang zu Daten in der *Cloud*, um beispielsweise politische Aktivitäten zu überwachen.

Einwilligung

Es ist zweifellos der Fall, dass Einwilligung im Datenschutz sehr wichtig ist. Wer nicht „nein" sagen kann, hat keine Macht. Trotzdem gibt es keine einfache und „richtige" Regelung in der Ära des Internets. Wenn man zehnmal am Tag „OK" klicken muss, ist das keine echte Wahl. Wie der Vorschlag sagt, muss die Einwilligung den BürgerInnen klare Informationen über die Datenbearbeitung einfacher zugänglich machen und simplere Methoden fördern, um explizite oder implizite Einwilligungen zurückzuziehen.
Und was ist Beweis genug? Wenn die Beweisregeln nicht streng genug sind, ist das eine Gefahr für die persönlichen Daten von BürgerInnen. Wenn aber die Beweisregeln zu streng sind, besteht die Gefahr, dass Firmen eher zu viele Daten sammeln werden, um sicher zu sein, dass sie diese Regeln respektieren können.

Privacy by design und privacy by default

Zwei ganz neue Prinzipien in der neuen Verordnung, die nicht explizit in der Richtlinie standen, sind *privacy by design* („Datenschutz durch Technik") und *privacy by default* („datenschutzfreundliche Voreinstellung"). Diese Prinzipien klingen bestimmt sehr gut. In der Praxis aber fürchte ich, dass sie nicht umgesetzt werden können. Artikel 23 Absatz 1 der vorgeschlagenen Grundverordnung zum Beispiel sagt, dass mit Rücksicht auf den Stand der Technik und die Implementierungskosten die Anforderungen dieser Verordnung genügen müssen und die Rechte der betroffenen Person gewahrt werden müssen.

Wenn es diesen Paragraphen gar nicht geben würde, sollte das dann heißen, dass die Anforderungen dieser Verordnung nicht respektiert werden müssten? Datenschutz muss nicht schon beim Design geplant werden. Stattdessen sagt die Verordnung nur, dass die Implementierung der Technik gesetzesgemäß durchgeführt werden muss: unter Berücksichtigung der Kosten.

Datenschutzfreundliche Voreinstellungen sind ein neues Prinzip, das wieder kaum neue Pflichten mit sich bringt. In der derzeitigen Richtlinie gibt es bereits ein Prinzip von Datensparsamkeit – dies gibt es nun auch in der neuen Verordnung. Eigentlich bedeuten „datenschutzfreundliche Voreinstellungen" nicht mehr, als dass so wenige Daten wie möglich bearbeitet werden dürfen. Anders gesagt – die Datenminimierung, die wir schon hatten. Die Tatsache, dass wir angeblich neue Prinzipien und neue Schutzmaßnahmen in der Verordnung haben, die aber in Wahrheit nicht neu sind, ist weniger harmlos als man sich erhoffen könnte. Die Datenschutzpolitik der EU wird bereits durch viele Unklarheiten geschwächt – weitere Unklarheiten führen dann dazu, dass der Datenschutz weiter geschwächt werden könnte. Das müssen wir dringend vermeiden.

Das Recht auf Vergessenwerden

Eines der im Moment am meisten besprochenen Themen in der Verordnung ist das sogenannte „Recht auf Vergessenwerden". Leider ist dies so dermaßen interessant für Journalisten, dass schon viel darüber gesagt, aber wenig verstanden wurde. Die Idee ist sehr positiv: Wenn Du einer Firma persönliche Daten gibst, hast Du das Recht darauf, das Löschen dieser Daten zu fordern. Der Vorschlag der Kommission – und die Reaktion darauf von der Industrie – lassen uns aber in einem Niemandsland zwischen dem, was die Kommission vorschlagen wollte und dem, was die Industrie fürchtet.

Anstatt ein einfaches Recht auf Vergessenwerden vorzuschlagen, spricht der Vorschlag der Kommission von „technischen Maßnahmen“ durch Dritte. Geldstrafen können für eine Firma anfallen, die nicht *„alle erforderlichen Schritte unternimmt, um Dritte von einem Antrag der betroffenen Person auf Löschung von Links zu personenbezogenen Daten sowie Kopien oder Replikationen dieser Daten gemäß Artikel 17 zu benachrichtigen“*. Der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten öffentlich gemacht hat, muss auch in Bezug auf die Daten, *„für deren Veröffentlichung er verantwortlich zeichnet, alle vertretbaren Schritte, auch technischer Art, um Dritte, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt“*, sicherstellen.

Das klingt gar nicht so schlecht, bis man sich fragt, was das zum Beispiel für Urheberrechtsverletzungen bedeuten würde? Schutz der Privatsphäre ist ein Grundrecht laut der Charta, aber ebenso ist der Schutz des geistigen Eigentums ein Grundrecht in der Charta. Was wird vom offenen und freien Internet übrig bleiben, wenn technische Maßnahmen zum Sperren, Löschen oder sonstigen Zugangserschwerungen zur Regel werden? Das Recht auf Vergessenwerden bedeutet nicht wirklich mehr als das Recht, eigene Daten zu löschen, was es schon in der jetzigen Richtlinie gibt und deswegen zu Unklarheiten und schwächeren Datenschutzrechten führen könnte. Artikel 17 muss also dringend überarbeitet werden. Die Regelung muss einfach sein! Firmen müssen nur für die Daten verantwortlich sein, über die sie Kontrolle haben. Es wird nur zu Einschränkungen unserer Freiheiten führen, wenn im Zeitalter des Internets, Firmen verantwortlich für Aktivitäten irgendeiner Art gemacht werden, über die sie gar keine Kontrolle haben.

Profiling

Profiling ist eine sehr komplizierte Frage und das nicht nur, weil dies sehr schwer zu regeln ist, sondern weil Staaten einen Interessenkonflikt haben. Auf einer Seite wollen sie die Grundrechte der Bürger gegen übermäßige Datenbearbeitung von Firmen schützen. Auf der anderen Seite aber benutzen Staaten immer mehr private Daten für angebliche Sicherheitszwecke. Je mehr *profiling* im privaten Sektor passiert, desto mehr Daten sind für Staaten vorhanden. Staaten benutzen immer mehr Daten von privaten Firmen für die innere Sicherheit – wir sehen das am Konflikt über die Vorratsdatenspeicherung, den Export von Finanzdaten an die USA, die Nutzung von Fluggastdaten für *profiling* und so weiter.

Ein sehr gutes Beispiel ist die Empfehlung des Europarates zum Thema *profiling*. Auf der einen Seite beinhaltet diese Empfehlung acht Artikel zum Schutz der Grundrechte im Bereich *profiling*. Auf der anderen Seite haben wir Artikel 6, der besagt, dass Staaten die wichtigsten Artikel der Empfehlung nicht umsetzen müssen, wenn *„in einer demokratischen Gesellschaft aus Gründen der nationalen Sicherheit, der öffentlichen Sicherheit, des Schutzes der monetären Interessen des Landes, der Verhütung oder Bekämpfung von Straftaten oder zum Schutz der betroffenen Personen oder der Rechte und Freiheiten anderer notwendig ist."*

Das kleine und übersehene Problem ist aber, dass *profiling* mittels bereits existierender Daten funktioniert. Anders gesagt, haben die Staaten wenig Interesse daran, die Sammlung von Daten zu verhindern, auch wenn es um *profiling* geht. Der Vorschlag der Kommission ist teilweise verbesserungsbedürftig. Erwägungsgrund 21 spricht von der Beobachtung des Verhaltens von Personen, während viele Beschlüsse im Bereich des *profiling* aufgrund von bestehenden Informationen gemacht werden und nicht unbedingt aufgrund Beobachtung. Artikel 20 Absatz 1 beschränkt sich lediglich auf rechtliche Auswirkungen und Fälle, in denen die Rechte des Bürgers in maßgeblicher Weise beeinträchtigt wurden – dieser Schutz ist für uns viel zu eng. Dies gilt auch für den Vorschlag, dass die Schutzmaßnahmen gegen *profiling* nur für Fälle gelten, in denen die Verarbeitung „rein" automatisch passiert.

Cloud Computing

Über den Wolken muss die Freiheit wohl grenzenlos sein. Unsere Freiheiten im Zeitalter von *Cloud Computing* riskieren eingeschränkt zu werden. Immer mehr Daten werden in Netzwerken gespeichert und nicht mehr auf einzelnen Rechner oder Servern in Büros. Die Verordnung erklärt das Verhältnis zwischen der Nutzung von personenbezogenen Daten in der Privatsphäre und den Pflichten der Cloudanbieter, wenn zum Beispiel Daten in einem sozialen Netzwerk oder in einem virtuellen Rechner gespeichert werden. Die Verordnung erklärt auch, wie die Pflichten verteilt sind zwischen, einerseits den für die Verarbeitung verantwortlichen Personen und andererseits den Auftragsbearbeitern. An sich sind die Fragen über die Regulierung von Cloud-Datenbearbeitung nicht kompliziert – die bereits existierenden Prinzipien müssen auch dort respektiert werden. Das Problem ist aber, dass Wolken keine Grenzen kennen.

Export von personenbezogenen Daten

Bereits bevor das Internet zu einem Teil unseres Alltags geworden ist, gab es große Probleme mit der Regulierung des Exports personenbezogener Daten. In der jetzigen Richtlinie gab es drei verschiedene Möglichkeiten, um Daten gesetzesgemäß ins Ausland zu schicken. Daten durften exportiert werden, wenn der Schutz im Drittland von der Kommission als akzeptabel erklärt wurde und wenn es ein spezifisches Abkommen mit dem Drittland gab sowie der Export aufgrund von für die Kommission akzeptablen Vertragsklauseln erfolgte.

Exporte, die aufgrund der Anerkennung von Drittländern erfolgten, haben bis jetzt keine zu großen Probleme verursacht. Der Haken ist aber, dass nicht viele Länder als angemessen anerkannt wurden. Das Problem mit Vertragsklauseln ist, dass sie nicht sehr transparent sind, was nicht erstaunlich ist, da es um Verträge zwischen privaten Firmen geht - auch wenn die einzelnen Klauseln durch die Aufsichtsbehörden anerkannt werden müssen. Das größte Problem aber ist das internationale Abkommen. Das berühmteste Beispiel ist das Abkommen mit den USA – das sogenannte *Safe Harbour* Abkommen. Studien zeigen, dass dieses Abkommen vollkommen daran gescheitert ist, seine Zwecke zu erreichen. Trotzdem will die Kommission dies nicht zugeben und es besteht keine große Hoffnung, dass dieses Problem durch die Überarbeitung der Richtlinie gelöst werden kann.

Kinderschutz

Ein neues Thema in der Verordnung ist der Schutz von Daten von Kindern. Diese neuen Regeln sind teilweise notwendig und positiv. Doch was passiert, wenn alle BürgerInnen Recht auf Datenschutz haben - aber mehr noch die Kinder? Hier besteht die Gefahr, dass eine Aufteilung des Datenschutzes in zwei unterschiedliche Niveaus, bei dem ein höherer Schutz für Kinder angestrebt wird, einen geringeren Schutz für den Rest der Gesellschaft mit sich bringen könnte, weil die Schwächsten ja bereits besonders geschützt sind.

Dass Daten von Kindern besonderer Schutz durch Artikel 33 gegeben wird, auf demselben Niveau wie genetische und biometrische Daten, ist positiv. Es ist auch positiv, dass bei Informationskampagnen von Aufsichtsbehörden der Schutz von Kindern besonders beachtet wird. Dann steht aber in Erwägungsgrund 53, dass das Recht auf Berichtigung von Daten *„besonders wichtig in Fällen ist, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gaben."* Das Recht war schon klar und eindeutig

für alle BürgerInnen vorhanden. Aber wenn man sagt, dass das Recht in bestimmten Fällen noch wichtiger ist, muss das logischerweise bedeuten, dass es für alle anderen manchmal nicht ganz so wichtig ist.

Berechtigtes Interesse

Das Konzept des „berechtigten Interesses" ist gar nicht neu, aber trotzdem sehr wichtig für eine moderne Datenschutzverordnung. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn sie eine von sechs Bedingungen (laut Artikel 6 der Verordnung) erfüllt. Eine von diesen Bedingungen ist, wenn die Verarbeitung zur Wahrung eines berechtigten Interesses geschieht und somit für den für die Verarbeitung Verantwortlichen erforderlich ist. Das kleine Problem ist dabei, dass es gar nicht deutlich ist, was ein berechtigtes Interesse überhaupt ist. Wie Ihr wisst, werden viele Daten von deutschen BürgerInnen in Irland verarbeitet, vielleicht wäre es interessant zu wissen, was der irische *High Court* darunter versteht.

Vor ein paar Jahren, hat der irische Internetanbieter Eircom ein sogenanntes Warnmodellsystem (auf Englisch *Three Strikes*) eingeführt. Hierbei sammelt eine Firma im Auftrag der Musikindustrie IP-Adressen im Internet von mutmaßlichen „Piraten". Diese Daten werden dann an Eircom weitergegeben. Eircom benutzt diese Daten, um Endkunden zu identifizieren und ihnen Warnbriefe zu schicken und schließlich ihre Internetverbindungen zu kappen. Und was hat das irische Höchste Gericht dazu gesagt? Dass es ein berechtigtes Interesse von Eircom, ist zu zeigen, dass sie das Recht durchsetzt! Hier ein weiteres Beispiel für das Problem der Definition von „berechtigtem Interesse": So sagte British Airways, das es erlaubt sei, Bilder von Kunden im Internet zu suchen und zu benutzen, weil dies Teil eines Dienstes ist und deswegen im berechtigten Interesse von British Airways.

Unter der neuen Verordnung wird dieses Problem noch verschärft. Da viele Aspekte der Verordnung etwas strenger sind als in der jetzigen Richtlinie, werden viele Firmen Interesse daran haben diese Lücke zu benutzen, um Datenbearbeitung zu rechtfertigen. Das haben sie mir schon selbst gesagt. Es ist also besonders wichtig, dass wir den vorgeschlagenen Text der Kommission hier erheblich verbessern. Von den parlamentarischen Berichterstattern wurde im EU-Parlament hierzu ein Arbeitspapier veröffentlicht, in dem dieses Problem erwähnt wird. Wir dürfen darauf hoffen, dass es bald gelöst wird.

Selbstregulierung

Teile der Kommission, die Vereinigten Staaten und große Teile der Industrie argumentieren für Datenschutz vor allem durch Selbstregulierung – und nicht ohne Erfolg. Was komisch, aber nicht besonders lustig dabei ist, ist dass die Industrie dieselben Argumente für mehr Selbstregulierung benutzt, die auch schon die Banken vorgebracht haben. Wie es jetzt dazu kommt, dass viele PolitikerInnen mitten in einer Krise, die teilweise durch mangelhafte Selbstregulierung verursacht wurde, nun bereit sind, wieder auf dieselbe Weise mit unseren Grundrechten zu experimentieren, ist mir völlig rätselhaft. Aber die Lage wird noch rätselhafter. Es wurde schon viel mit Selbstregulierung im Datenschutzbereich experimentiert und es gibt haufenweise akademische Studien, die zeigen, dass dies größtenteils zu mangelhaftem Schutz von Bürgerrechten führt.

Dies gilt vor allem für das *Safe Harbour* Abkommen mit den Vereinigten Staaten. Dies hat ein System von Selbst-Zertifizierung ins Leben gebracht, das völlig unfähig ist, den Schutz der Privatsphäre europäischer BürgerInnen zu gewährleisten. Trotzdem hat die Kommission dieses Abkommen unterschrieben und diese Selbst-Zertifizierung genügt, um Daten in die Vereinigten Staaten zu schicken. Nach viel Lobbyarbeit der USA wollen Teile der Kommission dies sogar ausbreiten statt zu begraben.

Schluss

Es ist noch viel mehr in der neuen Verordnung, was man hier hätte besprechen können. Ich hoffe aber, dass in meinem Beitrag dennoch klar geworden ist, wie wichtig dieser Vorschlag ist. Im Europäischen Rat, also bei den Mitgliedstaaten, wollen viele die Verordnung schwächen. Die Arbeitsgruppe, die daran arbeitet, beschäftigt sich normalerweise mit der Kooperation im Sicherheitsbereich. Manche TeilnehmerInnen haben deswegen wenige Sympathien für den Datenschutz. Manche europäischen Länder sind sehr sensibel für amerikanischen Druck. Im Parlament ist der Ausgangspunkt etwas positiver. Aber die ganze Industrie – die Finanzindustrie, die Onlineindustrie, die Pharmaindustrie und die Sicherheitsindustrie machen enorme Lobbyarbeit.
Wir haben das Unmögliche erreicht mit dem Vorschlag für Netzsperren in Brüssel. Wir haben das Unmögliche mit ACTA erreicht. Aber, ja, wir sprechen über einen Vorschlag. Den Vorschlag einer konservativen Kommissarin, mit dem der Großteil der LINKEN einverstanden ist. Ein guter Anfang, um wieder etwas Unmögliches zu erreichen.

Datenschutz in Sicherheit! Sinn und Zweck des Richtlinienentwurfs für den Bereich Polizei und Justiz

Sönke Hilbrans

Wortwahl und Zielstellung des Richtlinienentwurfs sind nahezu identisch mit derjenigen des Entwurfs der Datenschutzgrundverordnung. Was man hier heraus hören kann, zwischen den Zeilen, ist eine Binnenmarktideologie, die Terminologie und auch die Ideologie des ökonomischen Binnenmarktes, des gemeinsamen Marktes der früheren europäischen Gemeinschaften und heute. Das Projekt Europäische Union ist als Funktion von Datenschutz übernommen worden und eingegangen in eine Richtlinie, die jetzt im Sicherheitsbereich, das heißt im Kernbereich sowohl der hoheitlichen Gewaltausübung als auch des Schutzes der Grundrechte vor dem allmächtigen Staat angesiedelt ist.

Drei Geburtsfehler

Dass Binnenmarktideologie hier ernst gemeint ist, quasi der Kern des gesetzgeberisch Gewollten, muss uns zum einen aus bürgerrechtlicher Sicht provozieren und ist zum anderen leicht nachzuvollziehen an den Texten. So heißt es in der Begründung zur Richtlinie, dass der reformierte Datenschutzrahmen auf ein einheitliches hohes Datenschutzniveau gebracht werden soll, um das Vertrauen zwischen Polizei und Justizbehörden verschiedener Mitgliedstaaten zu stärken und damit zu einem freien Datenverkehr und zu einer wirksamen Zusammenarbeit zwischen Polizei und Justizbehörden beizutragen. Das liest sich im Artikel 1, Gegenstand und Ziele der Richtlinie, Absatz 2b: Ziel und Zweck ist es sicher zu stellen, dass der Austausch personenbezogener Daten zwischen den zuständigen Behörden in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten wird. Das muss man sich einmal ganz langsam auf der Zunge zergehen lassen. Ziel und Zweck eines als Datenschutzpaket verkauften Richtlinienentwurfs ist es, dass der Austausch von Daten zwischen den Zuständigen, gemeint sind Sicherheitsbehörden und Polizeibehörden in der Union, nicht aufgrund des Schutzes natürlicher Personen bei der Verarbeitung der Daten eingeschränkt oder gar verboten wird. Das ist sinnbildlich der Schritt in den Untergang.

Dies führt zu einer Datenschutznorm deren eigentliches Hauptziel es ist, nationale Unterschiede im Grundrechtsschutz, die den freien Datenverkehr zwischen den Behörden unterbinden können, abzubauen. Als ob freier Datenverkehr, nicht unterbunden von Behörden, ein Selbstzweck wäre. Sie wissen alle, am Grundgesetz geschult, dass die Dinge umgekehrt liegen. Freier Datenverkehr ist kein Selbstzweck, sondern – nein – jede Übermittlung, wie jede andere Verarbeitung personenbezogener Daten, orientiert er sich in jedem Einzelfall an einem konkreten Gesetz. Ein Gesetz, dass einen konkreten Zweck vorsieht und sicher stellt, dass der Vermittlungszweck auch die Interessen des Einzelnen und das Bedürfnis des Einzelnen, das heißt in seiner Privatsphäre geschützt zu bleiben, überwiegt. Datenschutz soll so gestaltet sein, dass er kein Hindernis mehr im europäischen Kontext der polizeilichen Zusammenarbeit darstellt, so die Botschaft der Richtlinie.

Ein zweiter bemerkenswerter Aspekt der Zielstellung der Richtlinie ist ihr Anwendungsbereich. Zum Gegenstand hat die Richtlinie die Verhütung und Verfolgung von Straftaten und die Vollstreckung von strafrechtlichen Urteilen. Das ist aus deutscher Sicht und deutscher Rechtstradition weder Fisch noch Fleisch. Denn das ist weder Polizeirecht noch Strafverfolgungsrecht, wie wir es kennen. Wenn sich der präventive Bereich einer Richtlinie auf die Verhütung von Straftaten beschränkt und nicht auf die allgemeine Gefahrenabwehr, dann haben wir es mit einer Regelung zu tun, die dem ersten Anschein nach zwar vollständig das Strafverfolgungsrecht abdecken soll, es aber nicht tut, weil sie in Wirklichkeit nur zu einem gewissen Teil das Polizeirecht abdeckt. Die Aufgabe der Polizei ist eben nicht nur die Verhütung, Aufdeckung und Prävention von Straftaten, sondern auch die Gefahrenabwehr. Es würde demnach ein Auseinanderfallen der Regulierungslandschaft im deutschen Polizeirecht zur Folge haben. Das ist der zweite Geburtsfehler, wenn man es so betrachten will. Denn im deutschen Wesen der Unterscheidung von Strafverfolgung und Gefahrenabwehr ist die Welt vielleicht nicht genesen, aber in jedem Fall liegt es quer zu der in Deutschland vorgefundenen Regelungslandschaft.

Der dritte Aspekt, der hier wichtig ist, kommt nicht aus der Unterscheidung und den Unterschieden, die wir im nationalen Recht vorfinden, sondern er kommt von der gemeinschaftsrechtlichen Seite her. Die Kommission meint, dass es eine Art Allzuständigkeit der europäischen Union für das Datenschutzrecht in der Union gibt. Dafür spricht Artikel 16 Absatz 2 des AEUV, der in der Tat so etwas in Verbindung mit dem Artikel 16 Absatz 1 vorzusehen scheint. Weil die Union diese Zuständigkeit hat, so deren Argumentation, hat sie auch im Bereich der polizeilichen und anderen Sicherheitsanwendungen die Zuständigkeit, als gäbe es dort keine inneren Schranken. Es gibt aber innere Schranken, das sind die generellen Beweisausnahmen für das Unionsrecht.

Von Relevanz ist der Bereich der sogenannten nationalen Sicherheit. Hatten wir eben noch von einer Allzuständigkeit der Union gesprochen, auch im Bereich der Polizei, so stellen wir jetzt im Bereich der nationalen Sicherheit fest, dass die Richtlinie konzeptionell gar nicht wirken kann. Nationale Sicherheit ist ein umstrittener Begriff. Wir würden ihm wohl entnehmen wollen, dass es bei nationaler Sicherheit darum geht, Gefahren von nationaler Bedeutung für die Mitgliedsstaaten von einer bestimmten Mindestschwere abzuwehren. Was darunter aber nicht gemeint ist, ist zum Beispiel allgemeine Kriminalität. Alles was Gegenstand geheimdienstlicher Tätigkeit oder von Staatsschutzkriminalität ist, würde nicht in den Bereich der nationalen Sicherheit fallen oder jedenfalls nicht ohne weiteres – also keine Terrorismusbekämpfung mit der Richtlinie. Hier ist schon ein erster Bereich, wo man zwar den Wunsch zu einem allgemeinen Datenschutzniveau im Sicherheitsbereich hat, aber eine wesentliche und in den Konturen unklare Bereichsausnahme zu verzeichnen ist.

Völlig aus dem Anwendungsbereich der Richtlinie scheinen weiterhin herauszufallen: Die Tätigkeit der Gerichte und die Strafverfolgung. Das ergibt sich jedenfalls dann, wenn man feststellt, dass die Richtlinie in ihren Normbefehlen den Gesetzgeber der Mitgliedstaaten adressiert. An einigen Stellen finden sich sogar Bereichsausnahmen für nationales Strafverfahrensrecht, wie die Tätigkeit der Gerichte und der Justizbehörden im engeren Sinne. Der Strafverfolger, vor allem die Staatsanwaltschaften, sollen von der Richtlinie, jedenfalls dem Normtext nach, nicht berührt werden. Das macht einen gewissen Sinn vor dem Hintergrund der jahrzehntelangen Diskussion um die innere Sicherheit in der EU. Das Strafverfahrensrecht bleibt in seinem Kern Gegenstand der Gesetzgebung der Mitgliedsstaaten. Es gibt Versuche, das nationale Strafverfahrensrecht der Mitgliedstaaten zu harmonisieren, was aber nicht im Rechtsrahmen des Datenschutzrechts stattfinden kann.

Es findet im Rechtsrahmen einer Harmonisierung der nationalen Gerichtsordnungen statt. Dazu gehört, endlich die europäische Menschenrechtskonvention auch in Frankreich durchzusetzen, um ganz elementare Beschuldigtenrechte gemeinschaftsrechtlich festzuschreiben, wie das Recht auf einen Verteidiger und das Recht auf Konsultation von Angehörigen oder einen Außenstehenden. Es gibt immer noch Mitgliedsstaaten, die glauben, diese auch in der europäischen Menschenrechtskonvention völlig unbestrittenen Rechte nicht anerkennen zu müssen.

Die Vereinheitlichung des Strafverfahrensrechts in der europäischen Union ist in den Anfängen und soll, wenn man sich den Normtext anschaut, nicht im Zuge der Richtlinie erfolgen. Was schwammig bleibt, vor allem wenn man sich die Erwägungsgründe und die Begleitpublikationen zu der Richtlinie anschaut, ist die Antwort auf die Frage:

Ist es wirklich ernst gemeint, dass das Polizeirecht oder das Recht der Sicherheitsbehörden in Europa mittels einer Richtlinie vereinheitlicht werden soll? Und wenn ja, geschieht das mit Ausnahme nachrichtendienstlicher Funktionen oder generell von Nachrichtendiensten? Oder soll sogar noch weniger erreicht werden? Das ist unklar.

Man arbeitet ja nicht ständig mit den Behörden der Nachbarstaaten der Union zusammen, sondern kümmert sich zunächst um den eigenen Kram und ein Raubmord in Leipzig bleibt ein Raubmord in Leipzig. Da muss man zuerst einmal mit niemandem außerhalb des Landes zusammenarbeiten. Wir wissen alle, dass Strafverfolgung im Wesentlichen ein nationales Geschäft ist und bei bestimmten Strukturen und Verdachtsmomenten eine ad hoc Kommunikation auch in Form der Rechtshilfe mit den Nachbarstaaten oder anderen Staaten stattfindet. Aber das ist nicht der Standardfall, lediglich die Ausnahme.

Nimmt man diese drei Probleme zum Ausgangspunkt, möchte ich die komplizierte Frage nach der Reichweite der Richtlinie am Ende nicht beantworten müssen. Das wird sowohl Gegenstand einer Verbesserung der Richtlinie sein, falls sie jemals in Kraft treten sollte, als auch Teil der anschließenden, herben Auseinandersetzungen.

Zumindest im Kern nachrichtendienstlicher Tätigkeit wird es auch keine Kooperation und Vereinheitlichung durch die Richtlinie geben. Dass es auch den Bereich der Sicherheitspartnerschaft mit anderen Nachbarstaaten und Mitgliedsstaaten gibt, in denen die Richtlinie sicherlich effektiv ist, ist das Eine. Das Andere ist, ob die Richtlinie auch den Ehrgeiz hat, die rein nationalen Probleme in der Rechtslandschaft der Mitgliedstaaten zu lösen.

Probleme der polizeilichen Datenverarbeitung – die Krise von Freiheit und Sicherheit

Wo liegen nun die Probleme der polizeilichen Arbeit und Zusammenarbeit aus bürgerrechtlicher Sicht? Hierbei denke man an „Handygate in Dresden“. Wo steht da die Richtlinie? Im nationalen Kontext würde wohl eine solche Richtlinie keinen Ehrgeiz haben, ein Handygate zu verhindern.

Im nationalen Kontext haben wir es mit einer Krise von Sicherheit und Freiheit zu tun. Und diese Krise ist Jahrzehnte alt. Wir kennen sie spätestens seit den Zeiten des Innenministers Kanther. Die Politik der inneren Sicherheit in den letzten zwei Jahrzehnten scheint sich zu einem der letzten Refugien, in der der Politiker wirklich noch Poli-

tiker sein darf, ausgewachsen zu haben. Politik der inneren Sicherheit ist ein Rückzugsgebiet des Staates in neoliberale Politik und ein großer Legitimationsfaktor derselben. Es gibt heute kaum einen Bereich, in dem nicht auch die Sicherheit eine Rolle spielt. Ausdruck der Krise von Sicherheit und Freiheit, ist eine Kaskade neuer Methoden der Ermittlungsbehörden.

So hat eine hinterher rollende Kaskade von Entscheidungen des Bundesverfassungsgerichtes im Bereich der inneren Sicherheit in den letzten 15 Jahren immer wieder aufgezeigt, wie man dem Wunsch der Politik, Sicherheit mit technischen Methoden und mit der Ausweitung von Eingriffsbefugnissen und Kooperationsmöglichkeiten zu erreichen, begegnen kann. Dieser Weg hat zu zahlreichen verfassungsrechtlichen Eingriffen geführt, so dass sich Gesetzgeber und Politiker nicht darüber beschweren brauchen, wenn am Ende schlechte Gesetze zustande kommen. Das Bundesverfassungsgericht (BVG) ist in die Rolle eines Ersatzkorrektur-Gesetzgebers gerutscht. Das regelmäßige Eingreifen des BVG, Massenkundgebungen wie die Freiheit-statt-Angst-Demonstrationen in Berlin, Handygate und Skandale im Bereich der Politik der inneren Sicherheit zeigen uns deutlich: Die Beziehung von Sicherheit und Freiheit und das Austarieren der Bedürfnisse des Kollektivs auf Sicherheit und der Anspruch des Einzelnen auf Erhaltung seiner Freiheitsräume, sind bis heute nicht sauber gelöst.

Mangelnder Rechtsschutz auf europäischer Ebene

Darüber gibt es auch keinen gesellschaftlichen Konsens in Europa. So alt die EU und die Politik der inneren Sicherheit ist – so häufig stellen die Mitgliedsstaaten fest, dass in ihre Souveränitätssphären eingegriffen wird, was immer wieder zu Rempeleien führt. Oft müssen wir als BürgerInnen registrieren, dass Dinge geschehen die uns ein Krisengefühl vermitteln. Die Einführung von EURODAC, des Schengener Informationssystems, die Kapazitäten von EUROPOL sind Beispiele dafür, dass das Vertrauen in die Organisation und den Schutz von innerer Sicherheit durch EU-Institutionen und auf der EU-Ebene keinesfalls gut aussieht. Man kann weder EUROPOL noch das Schengener Informationssystem vor dem Bundesverfassungsgericht verklagen und der bürgerrechtliche Anreiz, unter den erschwerten Bedingungen der EU Grundprinzipien des Menschenrechts und des Grundrechtsschutzes einzuklagen, einen Rechtsstreit zu führen, ist deutlich geringer.

Fehlende Transparenz in der internationalen Kooperation

Wo liegen die Probleme? Es gibt eine Krise in der Beziehung von Freiheit und Sicherheit – in der BRD ablesbar an den genannten Phänomenen. Krisenhafte Entwicklungen gibt es auch im internationalen Kontext, speziell im Bereich der Kooperation der Behörden. Es gibt wenig Transparenz. Was die Kollegen auf der anderen Seite der Grenze machen, weiß man in der Regel relativ selten. Es gibt zwar Instrumente um das aufzuklären, aber was mit Daten, die in einen anderen Mitgliedstaat transferiert werden wirklich geschieht, bleibt unbeantwortet. Die gegenseitigen Versprechungen und Zusicherungen über die Verwendung von übermittelten Daten mögen im Einzelfall effektiv sein, aber sie sind keine Garantie dafür, dass dabei nichts schief geht. Es gibt daher keine wirkliche Nachverfolgbarkeit.

Stattdessen gibt es Debatten darüber, wie im Falle einer gewissen neofaschistischen Terrororganisation aus Gründen des Schlendrians, schlechter Dokumentation und des Geheimnisschutzes keine zuverlässige und schon gar keine vollständige und kontrollierbare Kooperation zustande kommen konnten. Auch hier fehlt die Nachvollziehbarkeit.
Was es auch nicht gibt ist eine Synchronisierung des Verfahrensrechtes im Bereich der Strafverfolgung, der Gefahrenabwehr oder gar der Gerichtsverfahren. Damit komme ich zur Perspektive der Betroffenen: Für sie gibt es keinerlei Transparenz, wenn personenbezogene Daten durch eine Behörde ins Ausland transferiert werden. Sie werden weder benachrichtigt noch haben sie eine Vorstellung davon, was mit ihren Daten passiert. Keine Nachvollziehbarkeit gibt es auch bei EUROPOL.

Gibt es eine Krise in der Zusammenarbeit?

Daraus resultiert die Frage, ob wir es mit einer Krise in der Zusammenarbeit zwischen den Mitgliedstaaten aus polizeirechtlicher Sicht zu tun haben. Sicherheitsbehörden verweisen stets darauf, man könne und dürfe ja nicht effektiv mit den KollegInnen in Europa kooperieren, weil durch die unterschiedlichen Rechtsordnungen unklar ist, ob und wann man rechtmäßig oder rechtswidrig handelt, wenn man Daten übermittelt. Zu klären ist immer: Darf ich die Daten überhaupt übermitteln?

Als Strafverteidiger, der viel mit Behörden zusammengearbeitet hat, ist es mir in den letzten Jahren nicht vorgekommen, dass eine Strafverfolgung unterblieb, weil die Rechtskulturen in der EU nicht angepasst sind. Im Bereich der Strafverfolgung dominieren auf den Entscheidungsebenen bekanntlich nicht die Polizei sondern Staatsan-

waltschaften und Gerichte. Und es gibt unter dem Dach der EU und der Vereinten Nationen elaborierte Regelwerke zur Rechtshilfe. Es mag zwar ein bisschen dauern, doch es ist in aller Regel möglich, jede gewünschte polizeiliche Zusammenarbeit auf diesem Wege zu organisieren. Das gilt auch im Falle der Strafverfolgung. Es gibt daher keine Krise von großer Bedeutung in Bezug auf die polizeiliche Kooperation und die Strafverfolgung, die in mehr als nur in technischen Fragen läge. Es gibt faktisch nur einen Bereich, in dem sich unterschiedliche Rechtskulturen negativ auswirken, das ist der „rein polizeiliche" Bereich.

Das ist der polizeiliche Bereich, der nicht durch internationale Rechtshilfe in Strafsachen gekennzeichnet ist, in dem die Polizeibehörden ohne die Justiz tätig werden. Das ist in der Tat auch der Bereich, von dem ich meine, dass diesen die Richtlinie vereinheitlichen will, auch wenn insgesamt der Anwendungs- und Regelungsbereich keineswegs eindeutig ist. Neben der rein polizeilichen Kooperation bleibt für die Richtlinie noch der Bereich der Verhütung von Straftaten, also ein wesentlicher Teil der Gefahrenabwehr.

Datenverarbeitung und Gefahrenabwehr

Zuerst muss man fragen, was dort mit Daten geschieht? Handelt es sich doch hier um einen Bereich, in dem es nicht um die konkrete, drohende, festgestellte Gefahr geht und in dem in absehbarer Zeit und in einem bestimmten Ausmaß der Eintritt eines Schadens droht. Es geht vielmehr um die Erkennung von Mustern und Personenzusammenhängen, um daraus polizeiliche, nicht unbedingt strafrechtliche, aber eher kriminalistische Schlüsse zu ziehen.

Das Zweite ist die Sammlung von Daten auf Vorrat. Die Herstellung und Fütterung von Datenbanken als Vorsorge für künftige Strafverfolgung und die Anhäufung von Daten zur Gefahrenabwehr, wie sie dann auch unter wohlklingenden Dateinamen wie Gewalttäter LINKS, Gewalttäter RECHTS, WIKLAS und INPOL als Verbunddateien des Bundes und der Länder läuft. Darüber hinaus gibt es in jedem Bundesland eigene Datenbanken. Im Bereich Castor betreiben die Ostniedersachsen so etwas und sie werden das in Dresden (Funkzelle) auch haben. Die Sammlung auf Vorrat, die der Vorbereitung polizeilicher Maßnahmen dient, trifft den Anwendungsbereich der Richtlinie. Eine differenzierte Polizeirechts- und Datenschutzlandschaft in Europa führt dann tatsächlich dazu, dass hier nicht so effektiv und schlank zusammengearbeitet werden kann, wie gewünscht.

Ausdruck dieser Praxis ist die Errichtung gemeinsamer Datenbanken. Gemeinsame Datenbanken in deutschen, belgischen oder luxemburgischen Polizeibehörden zur Bekämpfung von Subventionsbetrug beispielsweise, zur Bekämpfung von Schleusergruppen oder von erkannten terroristischen Zusammenhängen. Die gemeinsame Analyse von Daten soll durch die Richtlinie erleichtert werden. Hier gibt es tatsächlich Hindernisse, die durch die bestehende datenschutzrechtliche Diversität unter den Mitgliedsstaaten der EU auftreten. Aber wir müssen uns auch politisch fragen: Wollen wir auf dieses Knirschen, dass sich, zumal durch Einschaltung europäischer Einrichtungen, wie zum Beispiel EUROPOL, auch lösen ließe, wollen wir darauf tatsächlich mit einem solchen Regelungsinstrument reagieren?

Welche Probleme löst die Richtlinie? Naht die Rettung für die Probleme oder naht sie nicht?

Sie naht nicht für die polizeiliche und geheimdienstliche Kooperation. Da greift die Zahnbürste der Richtlinie nicht auf den kranken Zahn. Sie naht auch nicht für die Strafverfolgung. Die Lösung für ein Problem, wenn wir denn ein Problem in Europa sähen, würde durch die Richtlinie, weil sie die Strafverfolgung nicht berührt, nicht eintreten. Sie regelt auch nicht die Eingriffsmethoden: die Vorratsdatenspeicherung, den Lauschangriff, die DNA-Analyse, Erhebung von DNA-Daten, Kennzeichenerfassung, zu allem kein Wort in der Richtlinie. Auch die Tätigkeit der Gerichte wird nicht betroffen.

Es gibt auch keine eigenen Aussagen der Richtlinie zum Verhältnis von Freiheit und Sicherheit. Die wenigen Sätze dazu sind nicht von Belang. Die Richtlinie bekennt sich dazu, dass sie zum Kern des bürgerrechtlichen Problems, der Abwägung und der In-Beziehung-Setzung von Freiheit und Sicherheit, kein Wort sagt. Damit verabschiedet sich die Richtlinie aus dem gesamten Spektrum ihrer Aufgaben, für die sie aus bürgerrechtlicher Sicht eigentlich stehen müsste. Wir würden als BürgerrechtlerInnen sagen: Dann können wir auch auf die Richtlinie verzichten.

Nur Insellösungen

Was die Richtlinie anbietet sind ein bis zwei Insellösungen, nach denen wir zumindest für den deutschen Kontext nicht gefragt haben. Dazu gehört eine leicht angedeutete Privilegierung besonders schützenswerter Daten, wie Gesundheitsdaten und Verweise zum Umgang mit gentechnischen Daten. Das ist für uns in Deutschland aber nichts wirklich Neues. Leistet die Richtlinie bezüglich der Rechte der Betroffenen und des

Datenschutzes etwas Substantielles? Meiner Meinung nach ist die Richtlinie da neutral. Sie macht nichts wirklich kaputt. Das nationale System der Rechte der Betroffenen wird weder blockiert noch irgendwie erweitert. Das nationale Verfassungsrecht bleibt in dieser Frage erhalten. Der Mehrwert ist also gering.

Zum Schluss kommen möchte ich mit einem richtigen Lob auf den Richtlinienentwurfsverfasser. Es gibt nämlich, genauso wie es die Grundverordnung vorsieht, in Zukunft und nach dem Willen des Verfassers des Richtlinienentwurfs, ein Recht auf Verbandsklage im Sicherheitsbereich. Das ist reines Dynamit. Damit kann demnächst die Deutsche Vereinigung für Datenschutz, der RAV, die Humanistische Union, das Komitee für Grundrechte und Demokratie oder die Rechtsanwaltskammer beim nächstbesten Verdacht auf irgendein Handygate das Beschwerderecht geltend machen und Verbandsklagen erheben. Und damit wäre tatsächlich in der Sicherheitslandschaft etwas erreicht, was es sonst nur in Israel gibt. Es ist sozusagen die Popularklage im Sicherheitsbereich möglich und dafür lohnt es sich. Datenschutz in der Hand des Einzelnen und Bürgerrechte des Einzelnen vor Gericht erstreiten, kostet wirklich Geld und das werden demnächst vielleicht Organisationen und Institutionen stemmen können. Da wird man sich warm anziehen müssen.

Söhnke Hilbrans, Karin Schuler

Datenschutz in Arbeit!

Karin Schuler

Ich spreche zu ihnen heute, meine Damen und Herren, als Vorsitzende der Deutschen Vereinigung für Datenschutz (DVD). Ich bin Beraterin für Personalräte und Betriebsräte und auch für betriebliche Datenschutzbeauftragte, das schon seit 25 Jahren. Ich bin von der Ausbildung her nicht Juristin wie mein Ko-Vorstandsmitglied Söhnke, sondern Informatikerin, habe also sehr viel Einblick in verschiedenste Arten von Unternehmen und würde das gerne nutzen, um anhand der Forderungen, die ich ihnen präsentieren möchte, etwas Futter für die Diskussion zu liefern.

Am Anfang würde ich gerne noch einmal die Frage stellen, warum wir uns überhaupt mit Arbeitnehmerdatenschutz so besonders befassen müssen. Was ist beim Arbeitnehmerdatenschutz eigentlich so anders als bei anderen Aspekten des Datenschutzes, der ja insgesamt ein Querschnittsthema ist und sich mit vielfältigen Aspekten befasst? Neben dem Verbraucherdatenschutz, wir haben eben den Bereich Justiz und Inneres gehört, gibt es noch vielfältige andere Lebensbereiche, in denen der Datenschutz eine Rolle spielt. Dennoch bin ich jemand, der für Arbeitnehmerdatenschutz viel Herzblut hat und ich bin offensichtlich nicht die einzige. Warum ist das so? Ich glaube, jedem ist sofort auch aus eigener Anschauung klar, dass im Beschäftigungsverhältnis besondere Kräfteverhältnisse herrschen und genau das ist auch letztlich der Grund, weswegen man sich damit befassen sollte, wie dieses besondere Kräfteverhältnis oder besser gesagt Missverhältnis zwischen Arbeitgeber und Arbeitnehmer zugunsten des Arbeitnehmers gestaltet werden sollte, insbesondere in Bezug auf den Datenschutz. Die Frage ist also, ist es erforderlich, dass ein Beschäftigter, der dem Arbeitgeber ja nicht auf gleicher Augenhöhe gegenüber tritt, im Bereich des Datenschutzes besonderen Schutz genießt, den er sich sonst auf andere Weise nicht verschaffen kann? Wir haben vielfältige Erfahrungen mit dem Arbeitnehmerdatenschutz, mit dem „Beschäftigtendatenschutz“, wie es zuletzt hieß. Wir haben nicht zum ersten Mal den Versuch erlebt, ein Gesetz für den Beschäftigtendatenschutz in Deutschland zu etablieren. Dieser Versuch ist zum wiederholten Male kläglich gescheitert, er ist sogar so glamourös gescheitert, sodass der DGB meiner Ansicht nach zu Recht gesagt hat: „das möge man doch bitteschön in die Tonne drücken.“ Denn was da herausgekommen ist, nachdem viele Bemühungen und viel Energie investiert wurden, ist wirklich das Papier nicht wert, auf dem es steht.

Es ist ernsthaft zu fragen, wie der Inhalt dieses Vorschlages eigentlich zu der Über-

schrift passt. Auch hier ging es im Wesentlichen um die Festlegung von Ermächtigungstatbeständen, also im Grunde darum, dem Arbeitgeber zu erlauben, bestimmte Daten seiner Beschäftigten auch zu ganz anderen Zwecken als zu Zwecken des Arbeitsverhältnisses zu verarbeiten. Es ging mitnichten in erster Linie um den Schutz der Betroffenen vor unrechtmäßiger Verarbeitung ihrer Daten im Arbeitsverhältnis, wie wir uns das wahrscheinlich als Freunde des Datenschutzes eher vorgestellt hätten.

Letzte Hoffnung EU

Wenn es denn im Nationalen nicht klappt, versuchen wir es doch mal auf EU-Ebene. Was wir da nun bekommen sollen, ist auch nicht das, was wir uns vorgestellt hatten. Im Grunde ist festzustellen, dass zum Beschäftigtendatenschutz zweierlei vorzufinden ist. Das eine ist eine sogenannte Öffnungsklausel, die den Nationalstaaten die Möglichkeit eröffnet, nähere Regelungen zum Arbeitnehmerdatenschutz zu erlassen, in eigenes nationales Recht zu gießen, sie verpflichtet sie aber nicht dazu. Der zweite Punkt, den man wohlmeinend dem Arbeitnehmerdatenschutz zuordnen könnte, ist eine Regelung, die sich im Bereich der Festlegung findet, wie man mit Einwilligungen zur Datenverarbeitung durch die betroffenen Personen umgehen kann. Die vorgesehene Regelung zur Einholung von Einwilligungen ist als Zulässigkeitsgrundlage für eine Datenverarbeitung etwas strenger und etwas restriktiver gefasst, als sie derzeit in unserem BDSG zu finden ist, aber es gibt auch einige Auslegungsfreiheiten. Wohlmeinend kann man sagen, dass etwas mehr Schutz herauskommt, wenn man es gut auslegt. So genau lässt sich das aber kaum sagen. Damit befinde ich mich eigentlich in einer recht komfortablen Position. Ich muss mich nicht an der Verordnung abarbeiten, ich kann die Position darstellen, die wir als DVD und auch mit anderen Datenschützern gemeinsam schon seit Längerem vertreten. Wir sind der Meinung, dass es in einer Regelung, sei sie national oder europäisch, bestimmter Grundanforderungen bedarf, die die besondere Position des Arbeitnehmers gegenüber dem Arbeitgeber in irgendeiner Form abmildern.

Sechs Vorschläge für den Arbeitnehmerdatenschutz

Daher möchte ich Ihnen gerne sechs Vorschläge für Mindeststandards machen und zur Begründung dieser Vorschläge jeweils Beispiele aus meiner alltäglichen Beratungspraxis anführen. Die erste Forderung lautet, dass Einwilligung im Arbeitsverhältnis nur in sehr begrenzten Fällen die Verarbeitung personenbezogener Daten ermöglichen darf. Das heißt, sie darf nur in sehr begrenzten Fällen als Zulässigkeitsgrundlage für Daten-

verarbeitung herangezogen werden. Das liegt daran, dass die Freiwilligkeit im Arbeitsverhältnis nur sehr schwer zu erzielen ist. Sie kann als Fiktion zwar einfach angenommen werden. Man kann sagen, jeder könne ja frei entscheiden. Das kommt aber der Realität nicht nahe, in der der Arbeitnehmer immer in Abhängigkeit von seinem Arbeitgeber ist, Angst hat, seinen Arbeitsplatz zu verlieren, Angst hat, benachteiligt zu werden, Angst hat, gemobbt zu werden, auch von Kolleginnen und Kollegen, wenn Konkurrenzsituationen nicht auflösbar sind, weil eine Beschäftigte irgendeine Einwilligung nicht erteilt hat. Dennoch gibt es durchaus positive Beispiele dafür, dass man sinnvolle Einwilligung auch im Arbeitsverhältnis sinnvoll einholen kann.

Ein Beispiel: Als speziell deutsches Problem führt die private Nutzung von Unternehmensressourcen dazu, dass der Arbeitgeber in eine Notlage kommt. Er kommt in die Lage, dass er durch die private Nutzung, die er gegenüber seinen Mitarbeitern zulässt, Telekommunikationsdienstanbieter ist und daher sehr strenge Vorgaben der Telekommunikationsgesetzgebung erfüllen müsste, dies aber aus Sicherheitsgründen und aus generellen Erwägungen des Betriebs eigentlich gar nicht tun kann. Er kann bestimmte Dinge nicht sofort löschen, Protokolleinträge nicht sofort löschen, wenn eine E-Mail angekommen ist. Was Telefonate angeht, kann er auch nicht sofort alles löschen, was im Unternehmensnetzwerk geschieht, weil er bestimmte Sicherheitsanforderungen erfüllen muss. Der Konflikt ist folgender: Entweder er erlaubt private Nutzung, dann muss er Anforderungen erfüllen, die er nicht erfüllen kann, oder er verbietet die private Nutzung. Diesen Konflikt kann man lösen, indem man dem Beschäftigten klar sagt, dass die private Nutzung erlaubt ist, aber nur dann, wenn er einwilligt, dass für die Behandlung der durch die private Nutzung entstehenden Daten keine besonderen Verarbeitungsprozesse eingeführt werden. Das heißt, bestimmte Daten werden nicht früher gelöscht, nur weil Daten über private Mails darunter sind. Wenn dem nicht zugestimmt wird, ist das nicht weiter schlimm. Die einzige Konsequenz ist, dass Unternehmensressourcen dann eben nicht privat genutzt werden können. Das ist ein Beispiel dafür, dass keine negativen Konsequenzen zu befürchten sind, wenn es richtig ausgestaltet wird. In so einem Fall kann man aus meiner Sicht mit Einwilligungen arbeiten, das ist aber auch einer der sehr seltenen Fälle.

Negativbeispiele gibt es viel mehr. Wenn im konzernweiten Adressbuch Fotos aufgenommen werden sollen, kann man das nicht mit Einwilligung rechtfertigen. Meine Erfahrung ist, dass wenn die Marketingabteilung entschieden hat, dass Fotos eingestellt werden, der Druck so groß ist, dass man nicht mehr von Freiwilligkeit sprechen kann. Von diesen Beispielen gibt es viele. Deswegen ist die erste Forderung, die Einwilligung zur Datenverarbeitung im Beschäftigungskontext nur in sehr begrenzten Fällen zu erlauben. Dazu muss sich ein Gesetz auch deutlich äußern.

Keine medizinischen Daten an den Arbeitgeber

Zweite Forderung: keine medizinischen Daten an den Arbeitgeber! Das klingt so einfach, aber der Teufel steckt im Detail. Medizinische Daten tauchen an viel mehr Stellen auf als man denkt. Simpelster Fall ist, dass der Betriebsarzt oder die Betriebsärztin einen Laptop oder einen eigenen Rechner bekommt, der dann an das Firmennetzwerk und die allgemeine Backuplösung angehängt wird. Natürlich werden, wenn etwas schiefgeht, die Administratoren helfend zur Seite stehen und Reparaturen vornehmen. Keine Daten an den Arbeitgeber weiterzuleiten heißt daher auch, die technischen Voraussetzungen dafür schaffen.

Ein zweites Beispiel. Stellen sie sich ein medizinisches Labor vor, indem die MTAs (Medizinisch-Technische Assistenten), in die Situation geraten, dass ihr eigener Arzt ihre Blutproben zufällig im eigenen Labor untersuchen lässt. Die medizinische Laborlandschaft in Deutschland ist gut aufgeteilt, es gibt nicht so viele Anbieter. Das führt dazu, dass die Auswahl in manchen Regionen nicht groß ist und die Daten dann im eigenen Labor landen. Diese Art Probleme treten schnell auf, wenn Mitarbeiter gleichzeitig Kunden sind. Wie geht man mit der Krankenschwester um, die im eigenen Krankenhaus operiert wird? Auch diese Spezialfälle müssen vernünftig durchdacht und geregelt werden.

Oder, eine Fachkraft für Arbeitssicherheit führt, und das ist sogar gesetzlich erforderlich, Unfallstatistiken. Die Unfälle lassen sich dann an diesen Statistiken ablesen, unter Umständen mit voller Namensnennung der Betroffenen und den Folgen. Das sind Diagnosedaten und damit medizinische Daten, die einem besonderen Schutz unterliegen. Oft macht sich niemand Gedanken darüber, was eigentlich außerhalb der betriebsärztlichen Betreuung an medizinischen Daten anfällt.

Datenflüsse in Konzernen begrenzen

Die dritte Forderung ist die Begrenzung von Konzerndatenflüssen, von Datentransfers innerhalb großer, transnationaler Konzerne. Das stellt im technischen Bereich eine Herausforderung dar. Wir wissen aus schlechter Erfahrung, dass die Freigabe von Konzernprivilegien letztlich einen Dammbruch darstellen würde, der es uns nicht mehr ermöglicht, an irgendeiner Stelle eine Grenze zum Schutz gegen unkontrollierbare Datenverarbeitung einzuziehen. Wenn gefordert wird, dass für Konzerne Privilegien in Bezug auf die Verarbeitung von Daten geschaffen werden, dann muss man sich auch überlegen, wie die wegfallenden Grenzen kompensiert werden sollen. Denn wenn ich

Konzerndatenflüsse grenzüberschreitend zulasse, dann unterwerfe ich diese Möglichkeiten den ökonomischen Gegebenheiten. Wer immer in irgendeiner Form beteiligt ist, juristisch, mit Anteilen, in GmbHs, er ist berechtigt und privilegiert, Daten an Konzernmutter oder Schwesterorganisationen weiterzugeben. Dann muss ich mich bei einer weltweiten Vernetzung fragen, wo eigentlich die Grenze ist.

Die Begehrlichkeiten von Konzernmüttern, durchzuregieren, seien es europäische oder internationale Konzerne, sind unglaublich groß. Ich hatte gerade einen Fall, wo es darum ging, dass die Konzernmutter, die in den USA sitzt, ganz offen damit argumentiert, dass sie Rechtspflichten aus US-amerikanischem Recht hat, denen sie nachkommen muss und die es erfordern, dass ihre Tochter in Deutschland Daten über ihre Arbeitnehmer liefert. Das ist eine Tendenz, die man sehen muss und wenn hier irgendetwas erleichtert wird, dann wird keinerlei Zweckbindung mehr einzuhalten sein.

Kontrolle stärken

Vierte Forderung: Wenn ich die Verarbeitung innerhalb europäischer Konzerne erleichtere, dann muss ich dafür sorgen, dass die interne und externe Kontrolle der Einhaltung der Datenschutzvorschriften mit den Konzernprivilegien Schritt halten. Eine Art Waffengleichheit ist zu schaffen. Wenn auf der einen Seite ermöglicht wird, dass die gesamte Datenschutzproblematik unter dem Aspekt des freien Datenflusses und der Nichtbehinderung der Wirtschaft gesehen wird, dann muss auch dafür gesorgt werden, dass die Vorschriften wirksam kontrolliert werden können. Es ist im Moment gerade in Deutschland so, dass in den Aufsichtsbehörden rein rechnerisch ein Mitarbeiter für Tausend Unternehmen vorhanden ist, der dafür sorgen müsste, dass in diesen der Datenschutz eingehalten wird. Soviel zur Größenordnung. Wir wissen, dass die meisten Aufsichtsbehörden in Deutschland mit ihrer Beratungs- und Auftragstätigkeit so dicht sind, dass sie einen Audit nur in sehr wenigen Bundesländern durchführen können. Das ist ein Zustand, den ich nicht für förderlich halte. Das muss auf jeden Fall geändert werden. Man muss dafür sorgen, dass die interne und externe Kontrolle von den Unternehmen überhaupt als Option wahrgenommen wird.

Ich bin vor zwei Jahren das letzte Mal gefragt worden: „ Frau Schuler, jetzt haben sie uns gesagt, wie alles sein müsste. Sagen sie jetzt mal, was es kostet, wenn wir nichts machen und wie groß die Wahrscheinlichkeit ist, entdeckt zu werden?“ Das zeigt sehr schön, wie wenig diejenigen, die Datenschutz nicht ernst nehmen wollen, ihn letztlich ernst nehmen müssen. Wir haben ganz viele Missstände, die flächendeckend bestehen und die Aufsichtsbehörden wissen das, kommen aber überhaupt nicht hinterher.

Das sind zum Beispiel *Whistleblowing-Systeme*, *Compliance* und die Diskussion darüber, ob die US-amerikanischen Mütter verlangen dürfen, dass zur Einhaltung von *Compliance*-Richtlinien teilweise datenschutzwidrige Systeme eingerichtet werden, bei denen in keiner Weise Datenschutzvorgaben erfüllt sind, die mit dem deutschen Recht in Einklang zu bringen sind. Wir haben ein großes Umsetzungsdefizit bei sogenannten Auftragsdatenverarbeitungsverhältnissen (ADV). Sowohl in Bezug auf die schlechte Ausgestaltung solcher Verhältnisse als auch in Bezug auf Missbrauch von ADV-Verhältnissen. Missbrauch insofern, dass innerhalb von Konzernstrukturen Dinge als ADV konstruiert werden, die sich bei näherer Betrachtung nicht als Auftragsdatenverarbeitung herausstellen. Das würde man auch bemerken, wenn man die Verträge und die tatsächliche Praxis untersuchen würde. Was mich daran am meisten ärgert, ist ein Missstand, über den seit Jahrzehnten diskutiert wird: Die Löschung von Daten.

Das was heute mit dem Erfordernis der Löschung verbunden wird, ist ein Witz. Wir haben das Erforderlichkeitsprinzip. Das heißt, dass man sich bei jedem Datum das man erhebt und speichert, von vornherein klar machen muss, wie lange man es aufbewahren muss, auf welcher Rechtsgrundlage dies erfolgt und wann diese Pflicht zur Aufbewahrung erlischt. Wenn man das in Unternehmen anspricht, wird man mit großen Augen angeschaut. SAP als einer der großen Anbieter ist nach vielen Jahren zu der Überzeugung gelangt, dass mit der Frage der Löschung von Daten aus ihren Systemen etwas professioneller umgegangen werden muss. Wenn sie sich Archivsysteme anschauen oder medizinische Laborsysteme, Backupsysteme, die so auf dem Markt sind: Löschen ist häufig überhaupt nicht vorgesehen. Man muss konsequenterweise sagen, dass Systeme, die auf dem Markt angeboten werden und kein Löschen ermöglichen, nicht datenschutzkonform einsetzbar sind. Sie dürften nicht zugelassen werden.

Ein weiterer großer Missstand ist die fehlende Beteiligung des Betriebsrates. Das ist ein Fall, der verdeutlicht, dass Datenschutz nicht nur eine Aufgabe für das Unternehmen und seinen betrieblichen Datenschutzbeauftragten ist, sondern auch eine Aufgabe im Rahmen der Mitbestimmung darstellt. Betriebsräte haben als Arbeitnehmervertretung bei allen Dingen mitzubestimmen, die zur Leistungs- und Verhaltenskontrolle geeignet sind. Das heißt, dass man davon ausgehen kann, dass jedes EDV-System, das in einem Unternehmen heute eingesetzt wird, mitbestimmungspflichtig ist. Viele glauben das nicht, aber ich lobe dann immer eine Tüte Gummibären aus, wenn man mir ein System nennen kann, das keine Daten speichert und nicht unter die Mitbestimmung fällt. Meine These ist, dass der Betriebsrat überall zu beteiligen ist, aber nicht beteiligt wird. Wenn er aber nicht beteiligt ist, ist das Mitbestimmungsrecht verletzt. Die Beschäftigtendaten, die trotz fehlender Mitbestimmung durch das Unternehmen verarbeitet werden, sind dann eben nicht ordnungsgemäß erhoben und verarbeitet worden.

Der Datenschutzbeauftragte muss einschreiten, Stopp sagen und das es so nicht geht. Hier verschränkt sich das Datenschutzrecht mit dem Mitbestimmungsrecht und diese Besonderheit wird nicht wahrgenommen. Ich habe es noch nicht erlebt, dass eine Aufsichtsbehörde aufgrund des nicht eingehaltenen Mitbestimmungsrechts selbst in sehr großen Systemen wie Krankenhausinformationssystemen, wo Beschäftigtenrechte mit Füßen getreten werden, ernsthaft den Stopp des Systems erwogen hätte. Wenn wir die Konzerndatenverarbeitung zulassen wollen, müssen wir an der Kontrollschraube drehen, das ist unerlässlich.

Verbindliche Normen für die technische Umsetzung

Fünfte Forderung. Wir haben ein Problem mit der Anpassung an die technologische Entwicklung im Datenschutz. Das ist ein seit Jahren ungelöstes Problem. Immer wieder wurden Versuche unternommen, bestimmte neue Technologien in das Gesetz hinein zu formulieren. Eines der Beispiele ist die Videoüberwachung, die es in die Gesetzgebung geschafft hat. Ich finde, dass das eine nicht-Fisch-nicht-Fleisch-Situation ist. Man muss sich überlegen, wie man es schafft, technologische Entwicklungen frühzeitig so in das Gesetzeswerk zu integrieren, dass man in einem Unternehmen auch damit arbeiten kann. Die Frage der Auslegungskompetenz in Bezug auf neue Technologien wie *Cloud Computing* ist für das Unternehmen, für betriebliche Datenschutzbeauftragte und für Betriebsräte ziemlich unklar. Es gibt eine Kakophonie der verschiedenen Gremien. Es gibt den Düsseldorfer Kreis, die Konferenz der Datenschutzbeauftragten, die Artikel 29-Arbeitsgruppe und demnächst die Stiftung Datenschutz. Jede Auslegung ist unverbindlich und im Zweifelsfall gerichtlicher Klärung unterworfen. Es wäre an dieser Stelle zu fragen, um Bewertungsunterschiede zu vermeiden die einem Unternehmen Knüppel zwischen die Beine werfen und dazu führen, dass die Akzeptanz von Datenschutz nicht sehr hoch ist, ob man in einem Gesetz oder in einer Verordnung ein Gremium normiert, dem man diese Auslegungskompetenz verbindlich zubilligt. Ich sage an dieser Stelle bewusst nichts über die Zusammensetzung oder die näheren Modalitäten. Die Grundidee ist, dass wir zu einem Verfahren kommen müssten, dass ähnlich den BSI-Grundschutzkatalogen in der Lage ist, auf neue technologische Herausforderungen so zu reagieren, sodass man einheitliche Auslegungsrichtlinien bekommt. Wenn sie in Schleswig-Holstein fragen, wie *Cloud Computing* gesehen wird, werden sie da womöglich eine andere Antwort bekommen als in Bayern. Ich rede hier nicht von der Ebene, auf der allgemein über Prinzipien befunden wird, ich rede hier von der tatsächlichen technischen Umsetzung.
Ich halte es für sinnvoller, wenn es ein direkt im Gesetzeswerk normiertes Gremium gibt, dass in der Lage ist, neue technologische Herausforderungen im Lichte der ge-

setzlichen Normierung zu prüfen und eine Handlungsempfehlung beziehungsweise eine verbindliche Auslegung zu erstellen, sodass man zu einer eindeutigen und für die Unternehmen auch nachvollziehbaren Beurteilung kommt. Stichwort ist best *practice*.

Das Verhältnis zu anderen Rechtssystemen

Letzter Vorschlag: Das Verhältnis zu anderen Wertsystemen ist zu klären. Es entstehen immer wieder im betrieblichen Alltag Situationen, bei denen vollkommen unklar ist, wie das Verhältnis von Datenschutzvorgaben zu anderen Wertsystemen zu sehen ist. Das Beispiel *compliance*-Forderungen habe ich eben schon genannt. Es gibt weitere, wie beispielsweise Qualitätsmanagement, Wirtschaftsprüfungsanforderungen, HGB, AO, Zoll, und Sanktionslisten-Scanning. Das machen Unternehmen, die meinen, sie müssten ihre Mitarbeiter gegen die Terrorlisten abgleichen, die die EU und USA erstellen, um zu verhindern, dass terroristische Vereinigungen mit Finanzen versorgt werden. Selbst Unternehmen, die das nicht tun wollen, bekommen dann vom Zoll keine vereinfachten Abwicklungsvorgaben mehr. Das heißt, dass sie vom Zoll gezwungen werden, ihre Mitarbeiter gegen EU-Sanktionslisten abzuprüfen. Das geschieht mit einer Häufigkeit, die sogar dem Innenministerium zu hoch ist. Das sind typische Konflikte für viele Arten von Normen.

Ein letztes Beispiel für einen derartigen Konflikt ist auch, wie ausländisches Recht bestimmte Datenverarbeitungen zulässig machen kann. Die amerikanische Mutterfirma, die ich eben erwähnt habe, ist der Ansicht, dass sie ihre Pflichten erfüllen müssen, weshalb sie von der deutschen Tochterfirma verlangt: „Liefere uns doch mal die Emails vom 1.1.2011 bis 6.12.2011 frei Haus, damit wir prüfen können, ob Verletzungen von *Compliance*-Richtlinien vorliegen. All das ist vorgekommen. Soweit meine sechs Punkte, die ich zur Diskussion stelle und von denen ich denke, dass sie in eine EU-Verordnung aufgenommen werden müssten.

Grundrecht Datenschutz

Lothar Bisky

Als Medienwissenschaftler und Kulturpolitiker bin ich natürlich vor allem Vertreter derjenigen, die offenbaren wollen, was hinter Daten und Informationen steht, z.B. Informationen über aktuelle Gesetzgebungsvorhaben und Diskussionen über linke Standpunkte und Ideen für eine solidarische und demokratische Informationsgesellschaft. Denn die Gesellschaft insgesamt ist im Zuge dieser technologischen Entwicklungen im Umbruch.

Die Digitalisierung von Teilen der Kommunikation, der Wirtschafts-, Arbeits- und privaten Welt bringt Chancen und Risiken mit sich. Sammlung, Speicherung, Auswertung, Erreichbarkeit und Weiter-Verwendung von Daten, auch personenbezogener Daten, wird einfacher, bequemer und teilweise billiger. Online-Banking, Online-Steuererklärung und –Einkauf, Routenplaner im Auto, Kommunikation per E-Mail oder in sozialen Netzwerken, Jobbörsen im Netz, jederzeit verfügbare Informationen, stets erreichbar zu sein und andere zu erreichen. Das hat durchaus Vorteile, weckt aber gleichzeitig Begehrlichkeiten bei privaten Unternehmen. Ich denke dabei unter anderem an Adresshändler, Inkassounternehmen, Werbung, Marktforscher, Banken u.v.m. BetreiberInnen einiger sozialer Netzwerke sind vielleicht das bekannteste Beispiel dafür. Staatliche Behörden sowie ArbeitgeberInnen können die neuen technologischen Möglichkeiten sinnvoll, aber auch zur Überwachung und Kontrolle der BürgerInnen ge- oder eben missbrauchen. Beides ist häufig nicht so weit von einander entfernt.

Politik und Gesetzgebung bewegen sich in diesem Spannungsfeld unterschiedlicher Interessen. Das deutsche Grundgesetz erhebt den Schutz persönlicher Daten nicht explizit in Verfassungsrang. Sehr wohl wird aber aus den Grundrechten nach Artikel 1 und 2 des Grundgesetzes ein „Recht auf informationelle Selbstbestimmung“ abgeleitet. Mit dem Vertrag von Lissabon, dort in Artikel 16 des Vertrags über die Arbeitsweise der EU, fand das „Recht [jeder Person] auf Schutz der sie betreffenden personenbezogenen Daten“ Eingang in die verfassungsgebenden Grundlagen der EU. Damit müssen wir arbeiten und sollten damit auch intelligent arbeiten. In der EU-Grundrechtecharta findet sich dieses Grundrecht in Artikel 8 wieder. Zugleich ist das Recht auf Sicherheit durch den Staat zu gewährleisten und in der EU-Grundrechtecharta verweist Artikel 6 auf die Gleichrangigkeit von „Freiheit und Sicherheit“. In den Debatten über den Schutz geistigen Eigentums oder soziale Netzwerke begegnen wir datenschutzrelevanten Fragen ebenso wie im Bereich der Strafverfolgung.

Gerade die digitalen Technologien erfordern nicht nur Gesetzesreformen sondern auch wiederum neue technische Ideen und ihre praktische Handhabung. Das zeigt sich zum Beispiel beim Ziel der Einrichtung eines „Rechts auf Vergessenwerden", also auf dauerhafte Löschung von Daten im Netz oder beim Recht auf „Rückgabe" bzw. Übertragbarkeit von Daten. Über diese Fragen ist hier ausführlich gesprochen worden. Eine weitere Frage, die sich stellt, ist folgende: Wo, in welchem Detail, auf welcher Ebene kann Datenschutz am besten geregelt und durchgesetzt werden? Die deutschen Bundesländer haben im März dieses Jahres im Bundesrat begründet, dass sie sowohl den Entwurf für die Datenschutz-Grundverordnung als auch die Richtlinie über den Datenschutz im Rahmen von Strafverfolgung und Justizkooperation für eine Überschreitung der Kompetenzen der EU halten.

Kann man aber in Zeiten des globalen und digitalen Datenaustauschs Datenschutz noch auf nationaler oder sogar noch den untergeordneten Ebenen regeln? Nach der „Panne", die dem Bundestag bei der Neufassung des deutschen Meldegesetzes unterlief, könnte man geneigt sein, dieser Ebene kein allzu großes Vertrauen vorzuschießen. Umso aufmerksamer muss natürlich verfolgt werden, dass die EU-weite Regelung nicht in ähnlicher Weise umgekehrt wird, wie es im Bundestag der Fall gewesen ist. BürgerInnen müssen etwaiger Datenweitergabe ausdrücklich und informiert zustimmen und ihre Erlaubnis auch zu späterem Zeitpunkt zurücknehmen können oder eine Datenweitergabe und -verarbeitung darf eben nicht erfolgen. Die Nichtweitergabe müsste also der Regelfall sein. Die Durchsetzung solcher Forderungen wird aber ein langer Kampf bleiben. Mit der Digitalisierung beginnen jetzt einige Probleme sichtbar zu werden und es werden weitere auftauchen, auf die unsere bisherigen Kulturtechniken nicht vorbereitet sind.

Eine weitere Schwachstelle in der deutschen Gesetzgebung zeigte die massenweise Funkzellenabfrage in Dresden im Februar 2011, bei der hunderttausende Verbindungsdaten von TeilnehmerInnen einer Demonstration und Unbeteiligten gespeichert und ausgewertet wurden und dieses Vorgehen letztlich als rechtmäßig beurteilt wurde.[3] Ungenügender Schutz von ArbeitnehmerInnendaten oder zumindest weit über das nötige Maß hinausgehende Erhebung solcher Daten ist beispielsweise auch im Europaparlament Thema von Auseinandersetzungen. Die Drohgebärde gegenüber abhängig Beschäftigten kann gewaltig sein: Wer fürchtet, keinen Arbeitsvertrag zu erhalten, unterschreibt eventuell mehr als sinnvoll oder sogar eigentlich zulässig ist. Umso mehr ist hier Politik in der Verantwortung, Regeln zu setzen und Betroffene zu unterstützen.

3 Stand von Juli 2012. In höherer Instanz wurde die Funkzellenabfrage letztlich doch als unrechtmäßig beurteilt.

Aber hier wie in vielen anderen politischen Auseinandersetzungen ist es eben so, dass wir Mehrheiten brauchen, um erfolgreich zu sein. Wir brauchen also auch mehr Linke. Anders ist nichts zu machen!

Eine EU-weite Regelung zum Datenschutz könnte in den genannten und weiteren Fällen möglicherweise Abhilfe schaffen. Wie schafft man aber, dass sich am Ende der bestmögliche Datenschutz durchsetzt und nicht etwa nur ein „kleinster gemeinsamer Nenner"? Dieses und andere Details werden im jetzt folgenden parlamentarischen Verfahren genau geprüft werden müssen. Wir müssen uns ansehen, ob mit diesen Gesetzgebungsakten beziehungsweise Änderungen daran das Abkommen zur Übermittlung europäischer Fluggastdaten an die USA vielleicht doch noch in seinen Auswirkungen beschränkt werden könnte. Gegen das so genannte PNR-Abkommen hat das Europäische Parlament lange Zeit Widerstand geleistet und ist dann doch am Ende mehrheitlich eingeknickt – übrigens gegen linke, grüne und liberale Stimmen. Hier zeigt sich auf der einen Seite, dass wir durchaus Schnittmengen mit andern Fraktionen im Europaparlament haben. Aber die erforderliche Stimmenanzahl für eine Mehrheit zu erhalten, ist eben harte Arbeit und nicht immer möglich.

Im Juli 2012, in der letzten Plenartagung des Europaparlaments vor der Sommerpause, ist das Anti-Piraterie-Abkommen ACTA von einer Mehrheit der Europaabgeordneten zu Fall gebracht worden. Conny Ernst, Initiatorin der Datenschutzkonferenz, trägt zusammen mit unserem Abgeordneten Helmut Scholz einen wichtigen Anteil an diesem Erfolg. Dies ist ein Beispiel dafür, dass auch die wenigen LINKEN Europaabgeordneten wirksam sind. Zentrale Sorge für die Bürgerinnen und Bürger waren Datenschutz und Freiheit im Internet. Mit der Ablehnung im Europaparlament konnte der Versuch abgewehrt werden, grundlegende Freiheiten und Grundrechte im Internet zu beschneiden. Fraglich ist natürlich auch hier: Für wie lange?

ACTA hätte EU und Mitgliedsstaaten darauf verpflichtet, für die Verfolgung von Verstößen gegen Copyright im Internet die Internetprovider in die Pflicht zu nehmen. Eine Folge hätte die Kontrolle des gesamten Datenverkehrs im Netz sein können. Weil mir die Anliegen von KünstlerInnen und AutorInnen besonders am Herzen liegen, sei mir der Hinweis gestattet: ACTA sollte den Besitzstand der größten Musik-und Filmkonzerne quasi per Staatsvertrag schützen. Es ging um Profitinteressen der Verwertungsgesellschaften, nicht um die Einkommenssicherheit der KünstlerInnen. Die Argumentation, dass hier Urheberrechte geschützt werden sollen, war ein ziemlich kleines Feigenblättchen.

Gefahren durch Terrorismus und Kriminalität sowie Probleme, die durch Korruption oder

Urheberrechtsverletzungen entstehen, gibt es natürlich sowohl online als auch offline. Die Notwendigkeit, hierfür Lösungen zu schaffen, darf aber nicht für die Legitimierung einer Überwachungsgesellschaft herhalten und auch nicht zur Beschränkung von Informationszugängen und Meinungsfreiheit – nicht in Deutschland und nicht in der EU.

Fragestellungen des Datenschutzes reichen in unzählige Bereiche hinein. Zu den bereits genannten lässt sich zum Beispiel auch die Frage hinzufügen, ob und wie „offene Daten" breiter und innovativ weiterverwendet werden können, ohne den Schutz personenbezogene Angaben zu verletzen. Dabei geht es um Informationen, die öffentliche Stellen produzieren, sammeln oder erwerben. Beispiele dafür sind Geoinformationen, Statistiken, Wetterdaten, Daten von öffentlich finanzierten Forschungsprojekten und digitalisierte Bücher aus Bibliotheken und auch Werke der Film-und Filmkunstgeschichte.

Gerade auch, wenn man – wie die LINKE – fordert, öffentliche Daten als für alle zugängliches Allgemeingut zu betrachten, stellt sich die Frage nach dem Datenschutz sehr deutlich. Die „netzpolitischen Eckpunkte" der Linksfraktion im Bundestag[4], das bereits bestehende Engagement der LINKEN im Europaparlament und anderen Parlamenten sind eine gute Basis für unsere Zielstellung, die digitale Gesellschaft in allen diesen Aspekten zu analysieren, kritisch zu begleiten und mitzugestalten. Eine moderne Linke im 21. Jahrhundert muss sich in diesem Bereich engagieren, nicht zuletzt im Interesse des Informationsproletariats, das sich in unseren Gesellschaften herausbildet. Mit unserer Datenschutzkonferenz haben wir einige wichtige konkrete Verhandlungsziele formuliert, die uns helfen werden, für Mehrheiten zu werben.

Es ist der Versuch, die Themenfelder Datenschutz, Bürgerrechte, digitale Gesellschaft, Netzpolitik, Urheberrechte – auch digitale Rechte – besser zu vernetzen. Wir formulieren damit den Anspruch, als ernstzunehmender politischer Partner in diesen Debatten auf allen Ebenen – Europa, Bund und Länder – noch deutlicher und kohärenter in Erscheinung zu treten.

Für den Beitrag zu diesen Vorhaben möchte ich allen Gästen und Experten sehr herzlich danken. Besonderer Dank gilt natürlich allen, die diese Konferenz auf die Beine gestellt haben und damit die Möglichkeit eröffnet haben, über dieses wichtige Thema – Datenschutz betrifft nun wirklich jeden – miteinander ins Gespräch zu kommen. Ich wünsche uns allen Erfolg bei den nun folgenden Verhandlungen!

4 Stand von Juli 2012. In höherer Instanz wurde die Funkzellenabfrage letztlich doch als unrechtmäßig beurteilt.

Ausgewählte Forderungen der GUE / NGL Fraktion im Europaparlament

Anwendungsbereich, Artikel 2
Die Verordnung soll auch für die Einrichtungen der EU gelten.

Räumlicher Anwendungsbereich, Artikel 3
Die Verordnung soll für alle Datenverarbeitung in der EU gelten und für alle Datenverarbeitung außerhalb der EU, wenn Daten von Menschen in Europa verarbeitet werden.

Zustimmung zur Datenverarbeitung, Artikel 7
Die Zustimmung muss freiwillig, informiert und ausdrücklich erfolgen.

Zustimmung soll in Arbeitsverhältnissen nicht gelten. Die Einwilligung bietet keine Rechtsgrundlage für die Verarbeitung, wenn zwischen der Position der betroffenen Person und des Datenverarbeiters ein erhebliches Ungleichgewicht besteht.

Die Zustimmung soll nur solange gelten, wie der Zweck, für den sie gegeben wurde, andauert. Wenn das nicht ganz klar gesagt werden kann, dann muss die Zustimmung einmal jährlich erneuert werden. Wenn das nicht ausdrücklich geschieht, dann ist die Zustimmung nach zwei Jahren automatisch beendet.

Besonders sensible Daten, Artikel 9
Die Verarbeitung personenbezogener Daten, aus denen die Rasse oder ethnische Herkunft, politische Überzeugungen, die Religionszugehörigkeit oder philosophische Anschauungen, sexuelle Orientierung oder Geschlechtsidentität, die Mitgliedschaft und Betätigung in einer Gewerkschaft hervorgehen, sowie von genetischen und biometrischen Daten, Daten über die Gesundheit oder das Sexualleben oder Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln soll verboten sein und nur möglich, wenn absolut notwendig.

Transparenz, Auskunft über Datenverarbeitung und Dokumentationspflicht, Artikel 11-14
Verarbeiter müssen Verarbeitung dokumentieren und den Betroffenen ausführliche Informationen geben. Dafür dürfen grundsätzlich keine Gebühren erhoben werden.

Datenportabilität, Artikel 18
Der Verarbeiter muss auf Anfrage alle Daten herausgeben. Das soll auch elektronisch möglich sein und muss dann in einem Dateiformat geschehen, das einem offenen Standard folgt und auch mit frei verfügbarer Software benutzt werden kann.

Einspruchsrecht, Artikel 19
Die betroffene Person muss ausdrücklich in einer verständlichen und von anderen Informationen klar abgegrenzten Form auf dieses Recht hingewiesen werden.

Einspruch soll auch gegen Datenverarbeitung möglich sein, die für Direktwerbung durchgeführt wird.

***Profiling,* Artikel 20**
Profiling soll nur unter strengen Auflagen in speziellen Fällen erlaubt sein.

Bei Entscheidungen, die auf profiling basieren, sollen Betroffene ihre eigene Sichtweise darlegen können.

Ein *profiling*, das unmittelbar oder mittelbar zur Folge hat, dass Menschen aufgrund von Rasse, ethnischer Herkunft, sozioökonomischen Status, politischer Überzeugung, Religion oder Weltanschauung, Mitgliedschaft und Mitarbeit in einer Gewerkschaft, sexueller Orientierung oder Geschlechtsidentität diskriminiert werden, oder das zu Maßnahmen führt, die eine solche Wirkung haben, soll immer verboten sein. Dasselbe gilt für das *profiling* im Beschäftigungskontext.

Sensible Daten nach Artikel 9 sollen nicht die Grundlage für *profiling* sein dürfen.

Bonitätsdaten bzw *profiling* sollten im Rahmen von Vertragsabschlüssen nur bei Nachweis besonderer Zahlungsausfallsrisiken verwendet werden dürfen.

Für die Prognose des Ausfallrisikos dürfen nur tatsächlich bonitätsrelevante Personendaten, wie Zahlungsanstände und Insolvenzdaten, benutzt werden.

Werden Scoringmethoden benutzt, so müssen sie zu wissenschaftlich stichhaltigen Ergebnissen führen.

Die Anbieter und Nachfrager von Bonitätsdaten müssen transparent vorgehen. Verbraucher sollten über die benutzten Daten, den Einsatz von Scoringmethoden u.a. informiert sein. Bonitätsdaten müssen aktuell und richtig sein.

Betrieblicher Datenschutzbeauftragter, Artikel 35
Datenschutzbeauftragter soll für alle Unternehmen und Stellen verpflichtend sein, wenn Daten von mehr als 500 Personen im Jahr verarbeitet werden oder Betroffene mit der Datenverarbeitung überwacht werden.

Arbeitnehmervertretungen sollen bei der Benennung des Datenschutzbeauftragten konsultiert werden.
Wird ein Datenschutzbeauftragter vorzeitig entlassen, muss das gegenüber der Aufsichtsbehörde begründet werden.

Datentransfers in Staaten außerhalb der EU, Artikel 40-44
Transfers in Drittländer, deren Recht ausdrücklich eine Verarbeitung vorsieht, die nach der Verordnung rechtswidrig wäre oder die sonst mit den Grundrechten unvereinbar ist, soll verboten sein.

Sogenannte berechtigte Interessen des Datenverarbeiters sind keine ausreichende Rechtsgrundlage für die Verarbeitung, wenn die Daten in Länder außerhalb der EU übertragen werden.

In Länder, die kein geeignetes Datenschutzniveau haben, sollen Daten nur nach ausdrücklicher und freiwilliger Zustimmung übertragen werden dürfen.

Firmeninterne Regelungen, wie *Binding Corporate Rules* sollen nur dann als Grundlage ausreichen, wenn sie auch außerhalb der EU rechtlich verbindlich durchsetzbar sind.

Datenzugriff durch ausländische Behörden, Anti-FISA, Artikel 43a
Ein Artikel, der die Weitergabe an ausländische Behörden beschränkt, soll unter dem Titel „Datentransfers, die nicht im Einklang mit dem Unionsrecht stehen" eingefügt werden, mit folgenden Forderungen:

1. Urteile von nicht-europäischen Gerichten und Entscheidungen von Verwaltungsbehörden dieser Staaten, die verlangen, personenbezogene Daten weiterzugeben, werden nur auf der Grundlage von Amtshilfe-Abkommen anerkannt und vollstreckt.
2. Verlangt ein solches Urteil diese Weitergabe, muss die zuständige Aufsichtsbehörde um vorherige Zustimmung gebeten werden.
3. Die Aufsichtsbehörde genehmigt die Weitergabe nur, wenn sie nach europäischem Recht erlaubt ist.
4. Die Aufsichtsbehörde unterrichtet die betroffene Person über das Ersuchen und die Genehmigung der Aufsichtsbehörde.

Aufsichtsbehörde und ihre Aufgaben, Artikel 46-54
Die Mitglieder der unabhängigen Aufsichtsbehörden für Datenschutz, die jedes EU-Land haben muss, sollen vom Parlament, nicht von der Regierung ernannt werden.

Über Datenpannen und Diebstähle soll ein öffentliches Register geführt werden.

Die Aufsichtsbehörde kann Whistleblowern, die auf unrechtmäßige Datenverarbeitung aufmerksam machen, bis zu 20% der daraus resultierenden Strafzahlungen als Belohnung zahlen.

Beschwerde bei der Aufsichtsbehörde, Artikel 73
Nicht nur Einzelpersonen, auch Verbände und Vereine sollen das Recht haben, Beschwerden gegen Datenverarbeitungen bei der Aufsichtsbehörde einzulegen. Das soll nicht an einen konkreten Fall geknüpft, sondern grundsätzlich möglich sein.

Sanktionen, Artikel 79
Die Aufsichtsbehörde soll Strafzahlungen verhängen können, die je nach Schwere des Vergehens bei Unternehmen bis zu 1%, 3% oder 5% des weltweiten Jahresumsatzes betragen können.

Arbeitnehmerdatenschutz, Artikel 82
Die Mitgliedstaaten sollen den Arbeitnehmerdatenschutz mit eigenen Gesetzen genauer ausgestalten können, allerdings nur in Übereinstimmung mit den Regeln der Verordnung.

Das Recht der Mitgliedstaaten, für den Arbeitnehmer günstigere Schutzvorschriften bei der Verarbeitung personenbezogener Daten im Beschäftigungskontext vorzusehen, bleibt unberührt.

Zusätzlich sollen die folgenden Mindeststandards gelten:
a) Die Verarbeitung von Beschäftigtendaten ohne Kenntnis der Arbeitnehmer ist unzulässig. Die Privat- und Intimsphäre der Arbeitnehmer ist jederzeit zu wahren;
b) Optisch-elektronische Überwachung der nicht öffentlich zugänglichen Teile des Betriebs, die überwiegend der privaten Lebensgestaltung des Arbeitnehmers dienen, insbesondere in Sanitär-, Umkleide-, Pausen-, und Schlafräumen, ist unzulässig;
c) Optisch-elektronische Überwachung der öffentlich zugänglichen Teile des Betriebs oder der nicht öffentlich zugänglichen Teile des Betriebs, die nicht überwiegend der privaten Lebensgestaltung des Arbeitnehmers dienen, wie Eingangsbereiche, Foyers, Büros, Werkhallen o. ä., sind nur zulässig sofern für die Sicherheit der Arbeitnehmer und des Betriebs zwingend notwendig;

d) Die Überwachung öffentlicher Teile des Betriebs sollte den Arbeitnehmer an seinem Arbeitsplatz soweit möglich nicht erfassen. Vor der Durchführung der Überwachung ist der Arbeitnehmer darüber zu unterrichten, wann und wie lange die Überwachungsinstrumente in Betrieb genommen werden;
e) Akustisch-elektronische Überwachung ist nur aus zwingenden Gründen der öffentlichen Sicherheit zulässig, etwa im Cockpit von Flugzeugen. Die heimliche Überwachung ist in jedem Fall unzulässig;
f) Jegliche Überwachung der nach Unionsrecht oder einzelstaatlichen Rechtsvorschriften und/oder Gepflogenheiten vorgesehenen Vertreter der Arbeitnehmer, einschließlich von Gewerkschaftsvertretern, ist in Bezug auf die Ausübung ihrer Vertretungstätigkeit unzulässig. Gleiches gilt für das sogenannte *blacklisting*;
g) Medizinische Daten von Beschäftigten, insbesondere solcher, die im Rahmen arbeitsmedizinischer Untersuchungen erhoben wurden, dürfen auch gegenüber dem Arbeitgeber nicht offenbart werden;
h) *Profiling* sowie Verarbeitungsvorgänge, die die permanente Kontrolle von Arbeitnehmern, deren Arbeitsleistung oder deren Verhalten zum Zweck haben, sind unzulässig. Dies gilt unabhängig von der eingesetzten Technologie.

Ist in einem Unternehmen nach dem Recht des Mitgliedsstaates eine Vertretung der Beschäftigten eingerichtet, so ist die Verarbeitung durch den Arbeitgeber nur zulässig, wenn die gesetzlich vorgeschriebenen Beteiligungsrechte eingehalten wurden.

Ist die Übermittlung von Beschäftigtendaten an Stellen außerhalb des Geltungsbereichs dieser Verordnung beabsichtigt, so ist in jedem Fall eine Prüfung durch den Datenschutzbeauftragten des Arbeitgebers vorzunehmen.

Unter Verstoß gegen diese Verordnung erhobene oder verarbeitete Daten über das Verhalten oder die Leistung von Beschäftigten dürfen weder gerichtlich noch außergerichtlich verwendet werden.
Arbeitnehmervertretungen sollen einbezogen werden in die Entscheidung:
a) zur Bestellung des betrieblichen Datenschutzbeauftragten;
b) zur Einrichtung und Anpassung datenverarbeitender Systeme;
c) die Formulierung von Binding Corporate Rules.

Die GUE/NGL Fraktion hat zahlreiche Änderungsanträge zu den Entwürfen der Kommission für Grundverordnung und Richtlinie unterbreitet, die hier aus Platzgründen in Vollständigkeit nicht aufgeführt werden können.

Zu berücksichtigen ist auch, dass viele Änderungsanträge zu den Entwürfen von den Berichterstattern eingebracht wurden, die wir inhaltlich unterstützen. Alle Änderungsanträge sind auf der Website des Europaparlamentes[5] abrufbar.

Cornelia Ernst (MdEP)

5 http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011%28COD%29#tab-0

Glossar

Accountability
Prinzip im Datenschutz und anderswo, das besagt, dass über jede Datenverarbeitung Buch geführt werden muss, sodass eine genaue Kontrolle möglich wird.

ACTA
Das Anti-Counterfeiting Trade Agreement, also Handelsabkommen gegen Produktfälschung, sollte unter tiefgreifenden Einschnitten in die Privatsphäre der Bürger unter anderem die Durchsetzung von Urheberrechten zwischen den reichsten Ländern der Erde angleichen. Das Europaparlament legte am 4.7.2012 sein Veto dagegen ein.

Artikel 29 Arbeitsgruppe
Das Gremium auf europäischer Ebene, an dem alle nationalen Datenschutzbeauftragten teilnehmen. Eingerichtet durch Artikel 29 der Richtlinie 95/46/EG, nach dem sie auch benannt ist. Sie überwacht die Anwendung europäischen Datenschutzrechts und berät bei neuen Gesetzesvorschlägen.

Auftragsdatenverarbeitung
Es ist bei Firmen und teilweise auch Behörden weit verbreitet, Daten nicht selbst zu verarbeiten, sondern an einen Dienstleister auszulagern. Dieser Dienstleister hat stark eingeschränkte Rechte in Bezug auf die Daten.

BDSG
Das deutsche Datenschutzgesetz.

Cloud Computing
Nicht ganz neue Technologie, mit der Dienste im Netz, wie Speicherplatz oder E-Mail angeboten werden. Die Daten liegen dabei irgendwo auf irgendwelchen Computern des Anbieters und können über das Internet von überall abgerufen werden. Deshalb ist oft nicht klar, welches Datenschutzrecht gilt. Da die meisten Anbieter von Cloud-Diensten in den USA sitzen, ist die Frage meist, ob amerikanisches oder europäisches Recht angewendet werden muss.

Code of conduct
Ein Verhaltenskodex.

Data breach
Ein Vorfall, der die Vertraulichkeit der Daten in Frage stellt. Kann die Folge eines Einbruchs, Unfalls oder schlechten Managements sein.

Datenschutzbeauftragte
In der EU ist es für die Mitgliedstaaten verpflichtend, eine unabhängige Aufsichtsbehörde für den Datenschutz einzurichten. In Deutschland existieren 17 dieser Behörden, jeweils eine pro Bundesland und eine im Bund.
In Deutschland, nicht aber im Rest der EU, sind Unternehmen und Behörden verpflichtet, einen betrieblichen Datenschutzbeauftragten zu haben. Dieser ist keine Aufsichtsbehörde, sondern hat innerhalb des Unternehmens eine beratende Funktion und ist Ansprechpartner für die Aufsichtsbehörde.

Datenschutzbeauftragtenkonferenz
Das Gremium in Deutschland, wo sich die Datenschutzbeauftragten der Länder und des Bundes treffen, austauschen und ihre Arbeit koordinieren.

EDPS
Der Europäische Datenschutzbeauftragte (European Data Protection Supervisor) ist die Aufsichtsbehörde für die europäischen Institutionen. Zudem hat er eine beratende Funktion bei allen europäischen Gesetzgebungsprozessen, die Auswirkungen auf den Datenschutz haben.

EuGH
Der Europäische Gerichtshof mit Sitz in Luxemburg ist für die Anwendung von EU-Recht zuständig.

Eurojust
Eine EU-Agentur mit Sitz in Den Haag, deren Aufgabe die Koordinierung von Strafverfahren auf europäischer Ebene ist. Jeder Mitgliedstaat entsendet einen Vertreter.

EURODAC
Datenbank, die die Fingerabdrücke von Asylantragstellern speichert. Ursprünglich eingerichtet, um zu verhindern, dass dieselbe Person mehrerer Asylverfahren anstrengen kann.

Europäische Bürgerinitiative
Neues europäisches Instrument, mit dem mit Hilfe von 1 Million Unterschriften europaweit eine politische Forderung an die EU herangetragen werden kann.

Europol
Die europäische Polizeibehörde ist eine EU-Agentur mit Sitz in Den Haag. Ihre Aufgabe ist vor allem der Austausch von Informationen und die Koordinierung von Ermittlungen bei schweren grenzüberschreitenden Straftaten.

FISA Act
US-Amerikanisches Gesetz, das dem Namen nach eigentlich der Gegenspionage dient. Es ermöglicht den amerikanischen Sicherheitsbehörden einen leichten Zugriff auf die Daten großer Internetfirmen, wie Google, Facebook und Amazon.

forum shopping
Wörtlich „auf dem Marktplatz einkaufen". EU-Jargon für die Tendenz von großen Unternehmen, sich dort in der EU niederzulassen, wo die für sie günstigsten Bedingungen herrschen. Meist geht es um Steuern, aber auch um die Rolle von Regulierungs- und Aufsichtsbehörden.

Grundrechtecharta
Die Charta der Grundrechte der Europäischen Union ist mit dem Lissabon-Vertrag Teil des Primärrechts der EU geworden. Enthalten sind Grund- und Menschenrechte, wie sie im Prinzip auch im Grundgesetz oder in der Europäischen Menschenrechtskonvention anerkannt sind, auch wenn diese nicht völlig identisch sind. Sie ist für die Institutionen der EU und für das EU-Recht verbindlich.

INDECT
Ein von der EU finanziertes Forschungsprogramm. INDECT soll es ermöglichen, in Echtzeit Informationen aus verschiedenen Quellen, wie Überwachungskameras und Internet zu gewinnen, um so „auffälliges Verhalten" erkennen zu können. Insbesondere bei DatenschützerInnen und BürgerrechtlerInnen gibt es harsche Kritik.

IP-Adresse
Eindeutige Adresse eines jeden Computers, der Teil eines Netzwerkes wie des Internets ist.

OECD
Organisation für Entwicklung und wirtschaftliche Zusammenarbeit ist eine internationale Organisation, die offiziell für Demokratie und Marktwirtschaft eintritt. Die 34 Mitglieder sind unter den reichsten Ländern der Erde.

PATRIOT Act
Der Patriot Act ist das amerikanische Anti-Terrorgesetz vom Oktober 2001 und damit der Kern der entsprechenden amerikanischen Gesetzgebung in der Folge des 11. September 2001. Es ermöglicht, vielfältige Datenverarbeitung bei extrem niedriger gerichtlicher Aufsicht.

Personenbezogene Daten
Fachbegriff im Datenschutz. Nur personenbezogene Daten fallen unter den Datenschutz. Gemeint ist jede Information, die sich auf eine identifizierte oder identifizierbare Person bezieht.

PNR
Eigentlich Passenger Name Records, gemeint sind Datensätze von Flugzeugpassagieren. Sie können über 20 verschiedene Einzelinformationen enthalten, darunter auch Essenswünsche im Flugzeug oder gebuchte Hotelübernachtungen. Die USA, aber auch andere Staaten benutzen die PNR um mithilfe von profiling nach bis dato unauffälligen „Verdächtigen" zu suchen.

profiling
Sammelbegriff für meist statistische Analyseverfahren, bei denen in riesigen Datensätzen bestimmte Verhaltensmuster gesucht werden mit dem Ziel, „unbekannte Verdächtige" zu finden. Kommt auch bei sog. Kredit-scorings zur Anwendung.

Prüm-Entscheidung
Überführt den Prümer Vertrag in EU-Recht. Prüm dient dem Austausch von polizeilichen Daten zur Bekämpfung von Terrorismus, grenzüberschreitender Kriminalität und Migration. Die meiste Bedeutung hat der Austausch von genetischen Daten zwischen den Ländern.

Polizeiliche und justizielle Zusammenarbeit in Strafsachen (PJZS)
Vor dem Lissabon-Vertrag die sogenannte „dritte Säule" der EU, neben den Europäischen Gemeinschaften und der gemeinsamen Außen- und Sicherheitspolitik. In dem Bereich war keine Mitentscheidung des Europaparlaments vorgesehen. Der Vertrag von Lissabon schaffte die Säulenstruktur ab und führte die Mitentscheidung für die PJZS ein.

Primärrecht
Die rechtlichen Grundlagen der EU und des Europarechts. Wichtigste Teile heute sind der EU-Vertrag und der Vertrag über die Arbeitsweise der Europäischen Union, die auch einfach nur „die Verträge" genannt werden.

Rahmenbeschluss 2008/977/JI
Beschluss im Rahmen der PJZS, der den Austausch von personenbezogenen Daten in der Polizeiarbeit regelt. Das Schutzniveau des Rahmenbeschlusses wird allgemein als sehr schwach angesehen. Soll durch die vorgeschlagene Richtlinie verbessert und ersetzt werden.

Richtlinie
Eine Form von europäischem Gesetz. Eine Richtlinie gilt nicht sofort in den Mitgliedstaaten, sondern muss innerhalb einer Frist in nationales Recht umgesetzt werden.

Richtlinie 95/46/EG
Die bewährte Datenschutzrichtlinie von 1995, gilt als Meilenstein im europäischen Datenschutz. Sie soll im Rahmen der Datenschutzreform durch eine Verordnung ersetzt werden.

Richtlinie 2002/58/EG, e-privacy Richtlinie
Regelt den Datenschutz in der elektronischen Kommunikation, also vor allem zwischen Internetprovider und Kunde. Als Grundregel darf der Provider eigentlich nur an Daten speichern, was für die Rechnungsstellung notwendig ist.

Safe Harbour Abkommen
Ein Abkommen zwischen EU und USA zum Datenschutz. Die Richtlinie 95/46/EG verbietet den Datentransfer in andere Staaten, wenn es kein ausreichendes Datenschutzniveau gibt. Amerikanische Firmen können sich unter Safe Harbour („sicherer Hafen") zertifizieren, dann ist der Transfer europäischer Daten zu dieser Firma legal.

Sekundärrecht
Im Gegensatz zum Primärrecht der EU ist das Sekundärrecht die Gesamtheit der Regeln, die auf Grundlage der Verträge beschlossen wurden, also alle Richtlinien, Verordnungen und Entscheidungen.

SIS, SIS II
Das Schengener Informationssystem der ersten bzw. zweiten Generation. Europaweite Datenbank, die bei Grenzkontrollen zum Einsatz kommt, enthält u.a. gesuchte Personen und gestohlene Fahrzeuge.

SWIFT
Eigentlich eine belgische Firma, die internationale Überweisungen abwickelt. Gemeint ist aber das Abkommen zwischen EU und USA, das den USA im Rahmen ihres TFTP-

Programms (Programm zur Aufspürung der Finanzierung von Terrorismus) ermöglicht, die Daten von SWIFT einzusehen und zu verarbeiten.

Three strikes
Gemeint ist damit allgemein ein Modell, mit dem bei zwei Verstößen verwarnt wird und beim dritten Verstoß eine automatische Strafe folgt. In verschiedenen Staaten wurden solche Modelle diskutiert und zum Teil auch eingeführt, um Urheberrechtsverstöße zu ahnden. Dabei ging es immer um illegale Downloads, die Strafe ist üblicherweise der temporäre Verlust des Internetzugangs.

Verordnung
Eine Form von europäischem Gesetz. Gilt sofort und unmittelbar in den Mitgliedstaaten und muss nicht eigens in das nationale Recht übertragen werden.

Verordnung (EG) 45 / 2001
Regelt den Datenschutz bei Verarbeitung personenbezogener Daten durch die EU-Institutionen und erschafft das Amt des Europäischen Datenschutzbeauftragten.

Vertrag von Lissabon
Bisher letzte Überarbeitung des Primärrechts der EU. Besteht aus dem EU-Vertrag, dem AEUV und der Grundrechtecharta.

Vertrag über die Arbeitsweise der Europäischen Union, AEUV
Nach dem Lissabon-Vertrag der Nachfolger des früheren EG-Vertrags. Der Inhalt sind Details, wie die EU zu welchen Themen und in welchem Umfang entscheiden kann und mit welchen Verfahren Entscheidungen getroffen werden.

Die Verträge
Das Primärrecht der EU.

VIS
Das Visa-Informations-System ist eine Datenbank mit den Daten, die bei Visa-Anträgen für die EU erhoben werden, darunter auch Fingerabdrücke.

Vorratsdatenspeicherung, Richtlinie 2006 / 24 / EG
Die Richtlinie zur Vorratsdatenspeicherung verpflichtet Telefon- und InternetanbieterInnen, die sog. Verkehrsdaten pauschal zu speichern, um Strafverfolgungsbehörden den Zugriff darauf zu erlauben. Das deutsche Gesetz zur Umsetzung wurde vom Verfassungsgericht in Karlsruhe verworfen.

Whistleblowing
Wörtlich „in die Pfeife blasen“. Whistleblower machen Informationen öffentlich, die Aufschluss über illegale Aktivitäten von Unternehmen oder Behörden geben. Damit sind oft strafbare Handlungen verbunden, wie etwa Geheimnisverrat o.ä. Deshalb gibt es in manchen Ländern Gesetze zum Schutz von Whistleblowern, deren Handlungen ja im Interesse der Gesellschaft stehen.

Gäste der Datenschutzkonferenz

We like Datenschutz! – Zu den Personen

Prof. Lothar Bisky (MdEP)
… von 2009 bis 2012 Vorsitzender der Konföderalen Fraktion der Vereinten Europäischen Linken/Nordisch-Grüne Linke (GUE/NGL), bis August 2013 Mitglied GUE/NGL; Stellvertretender Vorsitzender im Ausschuss für Kultur und Bildung; Stellvertretendes Mitglied in der Delegation für die Beziehungen zur der Volksrepublik China.
Er war von 1993 bis 2000 und von 2003 bis 2007 Bundesvorsitzender der PDS, von 2007 bis 2010 Ko-Vorsitzender der LINKEN; 2007 bis 2010 Vorsitzender der Europäischen Linken. Verstorben am 13.August 2013.

Dr. Cornelia Ernst (MdEP)
… ist seit 2009 für DIE LINKE als sächsische Europaabgeordnete tätig sowie Co-Vorsitzende der Delegation DIE LINKE im Europaparlament; Mitglied der Konföderalen Fraktion der Vereinigten Europäischen Linken/Nordisch- Grüne Linke (GUE/NGL); Mitglied im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres und Stellvertretendes Mitglied im Ausschuss für Regionale Entwicklung; zuständig für den Bereich Datenschutz in der Fraktion, insbesondere ACTA, SWIFT-Abkommen, PNR-Abkommen mit Australien bzw. USA, EU-PNR, Datenschutzpaket, SIS II sowie die Einrichtung der EU-Agentur für große IT-Systeme. Sie war von 1998 bis 2009 Landtagsabgeordnete in Sachsen und 2001 bis 2009 Landesvorsitzende der LINKEN in Sachsen.
Parlamentarische Arbeitsschwerpunkte: Datenschutz, Kohäsionspolitik, Migration sowie Gleichstellungspolitik.

Sönke Hilbrans
… ist Fachanwalt für Strafrecht. Mitglied im Vorstand des Republikanischen Anwältinnen und Anwältevereins e.V. (RAV); Stellvertretender Vorsitzender der Deutschen Vereinigung für Datenschutz e.V. (DVD); Cooperating Attorney ECCHR;
Schwerpunkte: Verwaltungsrecht und Datenschutzrecht.

Achim Klabunde
… ist Leiter der Abteilung für IT-Politik beim Europäischen Datenschutzbeauftragten. Vorher war er als Beamter in der Datenschutzeinheit der Generaldirektion Justiz und in der Generaldirektionen Informationsgesellschaft und Medien der Europäischen Kommission tätig, wo er während der Telekommunikationsreform 2009 für die Bereiche Privatsphäre und Vertraulichkeit von Kommunikation zuständig war.
Arbeitsschwerpunkte: Datenmanagement, Netzwerk-Planung, Datenschutz und IT-Sicherheit.

Lorenz Krämer
… studierte Philosophie und Politikwissenschaften an der Universität Bonn und ist seit 2010 parlamentarischer Assistent im Büro Dr. Cornelia Ernst (MdEP) in Brüssel.
Schwerpunkte: Datenschutz, Grenzpolitik, Migration.

Joe McNamee
… leitet das Brüsseler Büro von European Digital Rights (EDRi), dem Dachverband europäischer Datenschutz- und Bürgerrechtsorganisationen. Dazu gehört die Prüfung aller Vorgänge hinsichtlich der Bürgerrechte im Bereich des Datenschutzes der EU-Institutionen, d.h. Datenschutz, Vorratsdatenspeicherung, Zensur, Cyberkriminalität, PNR, SWIFT etc.
Schwerpunkte: Cyber-Kriminalität, Geistiges Eigentum und Telekommunikations-Politik.

Karin Schuler
… ist Vorsitzende der Deutschen Vereinigung für Datenschutz (DVD); Mitglied in der Gesellschaft für Informatik (GI) und im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung. Sie ist Expertin für Datenschutz und IT-Sicherheit, hauptsächlich für Projekte mit technischen und organisatorischen Fragestellungen, mit starken Bezügen zu Rechtsfragen aus Datenschutz und Mitbestimmung.

Prof. Lothar Bisky, Dr. Volker Külow (MdL, Die LINKE)

Impressionen

linXXnet-Aktion in der Leipziger Fußgängerzone zur Fachkonferenz der LINKEN„I like Datenschutz“ – am 14.7.2012 in Leipzig

Im Vorfeld der von der linken Fraktion im Europaparlament GUE/NGL und der Fraktion DIE LINKE im Sächsischen Landtag ausgerichteten Datenschutzkonferenz am 14.7.2012 in Leipzig fand in der Leipziger Innenstadt eine öffentlichkeitswirksame Aktion statt. PassantInnen trafen dort auf Schaufensterpuppen, die lediglich mit durchsichtigen Mäntelchen und Schildern (u.a. zu Facebook. Google, Handy, Email, Flugticket EU-USA ...) ausgestattet waren. Damit sollte auf den prekären Schutz persönlicher Daten in zahlreichen Lebensbereichen hingewiesen und für eine adäquate politische Regulierung des Datenschutzes plädiert werden.

linXXnet-Aktion in der Leipziger Fußgängerzone zur Fachkonferenz der LINKEN„I like Datenschutz“ – am 14.7.2012 in Leipzig

linXXnet-Aktion in der Leipziger Fußgängerzone zur Fachkonferenz der LINKEN„I like Datenschutz“ – am 14.7.2012 in Leipzig

Impressionen

Datenschutzkonferenz

Links nach rechts: Lorenz Krämer, Dr. Volker Külow, Cornelia Ernst, Klaus Bartl

Lorenz Krämer: Wissenschaftlicher Mitarbeiter, Büro Dr. Cornelia Ernst (MdEP)
Dr. Volker Külow (MdL,Die LINKE)
Dr. Cornelia Ernst (MdEP)
Klaus Bartl (MdL, die LINKE)

Datenschutzkonferenz

Joe McNamee

Datenschutzkonferenz

Gäste der Datenschutzkonferenz

Kontakt

Dr. Cornelia Ernst

Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres

In Brüssel:
Cornelia Ernst (MdEP)
Europäisches Parlament
ASP 6 F 154
Rue Wiertz 60
B-1047 Brüssel
Tel. +32 2 2837660
Fax: +32 2 2849660
Mail: cornelia.ernst@europarl.europa.eu
Wissenschaftliche Mitarbeiter: Lorenz Krämer
Mail: lorenz.kraemer@europarl.europa.eu

In Dresden:
Cornelia Ernst
Wahlkreisbüro / Europabüro Dresden
Schweriner Straße 50a
D-01067 Dresden
Tel. 0351/426 900 05
Fax: 0351/206 990 46
Mail: europa@cornelia-ernst.de

In Leipzig:
Europabüro im linXXnet Leipzig
Bornaische Straße 3d
D-04277 Leipzig
Tel. 0341/308 11 99
Mail: juliane.nagel@linxxnet.de

GUE/NGL
Vereinte Europäische Linke/Nordische Grüne Linke
Parlamentsfraktion · EUROPÄISCHES PARLAMENT

DIE LINKE.
IM EUROPAPARLAMENT