Tagung 23: „BIG DATA – Gefährdet die digitale Revolution unsere Demokratie?“

1) Arno Widmann, Journalist und Redakteur im DuMont-Verlag, Berlin: „Gefährdet die digitale Revolution unsere Gesellschaft? Müssen wir etwas tun? Können wir etwas tun?“

Arno Widmann, der als Redakteur des DuMont-Verlags tätig ist, u.a. für die Frankfurter Rundschau, hebt die digitale Revolution als wichtigstes Ereignis der letzten 20 bis 25 Jahre mit fundamentalen Wirkungen auf das wirtschaftliche und gesellschaftliche Leben hervor.
Für ihn als journalistisch tätige Person sei die digitale Revolution unmittelbar spürbar gewesen: Er bezeichnet sie sogar als das einschneidendste Ereignis [#alternativ: bzw. die prägendste Veränderung] in seinem beruflichen Leben. Da digitale Daten wesentlich schneller zu beschaffen seien, habe die digitale Verfügbarkeit von Informationen die Rahmenbedingungen seiner beruflichen Tätigkeit nicht nur erleichtert, sondern auch die Abläufe grundlegend beschleunigt. So konnten nun anstelle der zeitaufwändigen Beschaffung und Sichtung der internationalen Tagespresse themenbezogene Daten digital rasant zusammengestellt werden. Gleichzeitig wären solche digitalen Informationen aber auch für die Leser viel einfacher greifbar, die auf dieser Basis die journalistischen Veröffentlichungen unmittelbar mit anderen Informationsquellen abgleichen könnten, so dass die Zeitungen also nicht mehr so oft wie zuvor als einzige Basisinformationsquellen genutzt würden und die Leser eine deutlich kritischere und kontrollierende Haltung gegenüber medialen Veröffentlichungen einnehmen könnten. Hierdurch würden im Allgemeinen höhere Erwartungen an die journalistische Arbeit gestellt werden.
Widmann vergleicht das Ausmaß der Veränderungen, die durch die Digitalisierung angestoßen worden sind, mit der historisch vorangegangenen Welle der Elektrifizierung. Dieser Wandel im ökonomischen und gesellschaftlichen Leben habe sich zunächst so schleichend vollzogen, dass die einschneidenden und weitreichenden Konsequenzen anfangs kaum als „digitale Revolution“ erahnbar waren.
Der damals vorherrschende Revolutionsglauben unter linksrevolutionär Interessierten assoziierte eher Vorgänge der Dritten Welt, insbesondere in Lateinamerika, mit wegweisenden Entwicklungen hin zu einem radikalen Wandel, der sich weder an den Interessen der Großindustrie noch an der Realität in der DDR orientieren wollte, sondern hierzu einen alternativen Weg bieten sollte.
Hier übersah man die tiefgreifenden gesellschaftlichen Veränderungen, die sich allmählich über die digitale Revolution in kleinen Schritten selbst am eigenen Arbeitsplatz bemerkbar machten.
Faktisch wurde mit dem Aufkommen der digitalen Revolution das Industriezeitalter allmählich verdrängt – während das Produzieren, Sammeln, Verarbeiten und Konsumieren von Daten als Dienstleistung zunehmend an Bedeutung gewann. Diese Dienstleistungen basierten wiederum auf technischen und wissenschaftlichen Fortschritten in unterschiedlichsten Bereichen, durch die sich die Datenverarbeitung zunehmend beschleunigen und automatisieren ließ. So war vor etwa zehn Jahren noch eine mehrjährige Anstrengung notwendig, um die etwa drei Milliarden Basenpaare des Genoms zu identifizieren, während diese Leistung mittlerweile von einem hierauf spezialisierten Labor in nur einem Tag geleistet werden kann. Mit dem digitalen Angebot stieg auch die Nachfrage rasant an, wie die beispielsweise die 800 Millionen User veranschaulichen, die sich (#pro Tag?] einen Film herunterladen, der mehr als eine Stunde lang ist. Auch digitale Kommunikationsmedien wurden zeitnah überwiegend recht weitgehend angenommen, worauf etwa die ca. 400 Millionen twitter-Einträge pro Tag hindeuten oder die kaum vorstellbare Datenmenge von einem Petabyte (dies

entspricht einer eins mit 15 Nullen), die google pro Tag verarbeitet. Etwa 1200 Exabyte [## ohne Gewähr, BG], also eine unvorstellbar große Menge an Daten komme durch die digitale Verarbeitung aktuell auf, die erst durch Statistiken in ihrer Menge zu veranschaulichen und greifbar zu machen seien. Das Aufkommen dieser Datenmengen berge neue Gefahren: Einerseits entstünden neue Begehrlichkeiten, **Schlüsse auf spezifische Einzelne aus Datenkombinationen ziehen zu können**. Umfassender wirken die so entstandenen neuen Möglichkeiten, aufgrund statistischer Zusammenhänge statistisch begründete Bilder zu entwerfen und daraus Controlling-Regeln zu generieren, die zwingend gültige Kriterien dafür liefern sollen, weitgehende, von allgemein erwünschten Handlungsmöglichkeiten ausschließende Zugangsschranken festzulegen. Als viel zitiertes Beispiel sei hier etwa das Schufa-Scoring auf Datengrundlage der Wohngegend angeführt.
Somit würden also auf Grundlage statistisch häufig auftretender Datenkombinationen neue Regeln für die Exklusion von gesellschaftlichen Teilgruppen von ökonomischen Handlungsmöglichkeiten oder sonstigen angestrebten Lebensbedingungen und Optionen verbindlich aufgestellt.
Die Qualität des Wandels wird darin deutlich, dass nun **statistisch generierte, als relevant unterstellte Zusammenhänge als Entscheidungsgrundlage für gesellschaftliche Exklusionsregeln** dienen, die inhaltlich mitunter auch relativ willkürlich gewählt sein können. Die Gesellschaft erscheine nicht mehr, wie vor der digitalen Revolution, als eine Zusammenfassung von einzelnen Personen. Diesen Qualitätswandel verdeutlicht Widmann auch anhand einer Schrift Platons aus dem Jahr 370 vor Christi: Hier erzähle Sokrates ein Gleichnis über den ägyptischen Dämon [## Teut], der versuchte, den Pharao davon zu überzeugen, seine Kenntnisse der Schrift und der Mathematik im Volk zu verbreiten. Die Nachteile seiner Absicht verschwieg er: „Wer die Schrift erlernt, erlernt das Vergessen, denn die Erinnerung wird nicht mehr geübt werden; nicht für das Erinnern, sondern für das Gedächtnis wurde die Schrift erfunden. So entstehe nur die Einbildung, etwas zu verstehen, aber keine echte Weisheit, sie sind zu Dünkelweisen geworden und meinen nur, weise zu sein, sind aber keine echten Weisen geworden." Die Erkenntnisfähigkeit des Menschen werde also mit der zunehmenden Datenmenge zurückgesetzt, „die virtuelle Wirklichkeit ersetzt oft die reelle Wirklichkeit."
Den gesellschaftlichen Idealzustand umschreibt Widmann so: Eine Gesellschaft, die Wert auf den Einzelnen lege, sei eine Gesellschaft von Kuckuckseiern. Solch eine Gesellschaft möchte den Einzelnen nicht zurückführen und reduzieren auf das, woher er komme, die Herkunft bestimme hier nicht die Zukunft, die Zukunft müsse für jeden jeder Herkunft offen sein. (In solch einer Gesellschaft könnten somit wohl auch statistische, eindeutig erhebbare Merkmale kaum als zentraler Inhalt von Exklusionsregeln durchgesetzt werden.) Neben dieser Erscheinung und dem Grundrisiko der digitalen Revolution, statistisch basierte Zusammenhänge als Ausschlussregeln hervorzubringen – betont Widmann auch die Chance, die mit der digitalen Informationsplattform Internet verbunden ist: als Netzwerk zur Wissensgenerierung.
Unsere Aufgabe sei es, **„smart rooms"** zu schaffen, also die Gelegenheit, sich zu vernetzen. Dabei seien die smart rooms Teilbereiche des Internet, die jeweils Räume zur Wissensvermittlung und Meinungsäußerung geben. Das Internet sei nicht an sich ein smart room und müsse, um nicht schädlicher als nützlich zu sein, von uns in **smart rooms zerlegt werden, die sich gegenseitig widersprechen**.
Eine weitere Voraussetzung für eine positive Nutzung des Internet sei das **Recht auf anonyme Meinungsäußerung**, der Name des Verfassers darf nicht mit dem Gedanken verknüpft werden können. Gerade für die Äußerung nichtkonformer Gedanken müsse es smart rooms geben, in denen das Verbotene gesagt werden könne. Ohne diese Grundvoraussetzung ist das Internet die Fortsetzung der Tyrannei des Herrschenden.

Die Gefahr bestehe in dem Wissen, dass wir dem Netz geben, auch durch deutlich weniger unmittelbar wahrnehmbare Risiken der Wirtschaftsspionage. Dieser Risiken seien sich selbst Unternehmen nicht immer voll bewusst.
Durch das Internet werde die Möglichkeit geschaffen, jenseits von staatlichen Einflüssen sozialen Wandel anzustoßen und zu beschleunigen. Durch mitunter provozierende Veröffentlichungen im Internet wie beispielsweise auch durch international gepostete Kommentare auf you tube, werden gesellschaftliche Konsense oder gar Nationen herausgefordert. Das Internet helfe uns eventuell auch durch den Einfluss relativ exotischer Positionen, unsere Tabus zu entdecken und vielleicht neu zu beurteilen. Es könne unser Verhältnis zu uns verändern, unsere Einschätzungen dessen, was wir für richtig und falsch erachten.
Das Internet müsse von uns genutzt werden, um die Politik zu verändern, die selbst zum Täter werden könne. Wenn wir die Chance (gerade auch der anonymen) Einflussnahme über das Internet nicht nutzen, etwa um Missstände zu benennen, drohe das verbleibende Risiko, die Übermacht der gerade auch über das Internet generierbaren Big Data Nutzungslogik - auch etwa Stellungnahmen und Identitäten zu verknüpfen oder über Big Data statistisch begründete, gesellschaftlich verbindliche Regeln zu generieren - , sich zum „Totengräber der Gesellschaft“ zu entwickeln.

2) Alexander Sander, Geschäftsführer, Digitale Gesellschaft e.V. Berlin:
„Die Sicherheitsinteressen des Staates und die Sammelwut der Unternehmen konterkarieren die Idee des freien, unabhängigen Internets als Kommunikationsmedium für Alle“

Der Diplom-Politologe Alexander Sander stellt als Geschäftsführer der digitalen Gesellschaft e.V. Berlin die Ziele seiner Organisation vor, Bürgerrechte in einem freien Internet zu stärken. Dies werde überwiegend mittels Lobbyarbeit umgesetzt, sonst auch durch Kampaigning, also Projekte wie u.a. Demos.
Als Ausgangspunkt erläuterte Sander die Entwicklung der zunehmend als Begründung von weiteren angestrebten Kontrollmöglichkeiten im Internet herangezogenen Sicherheitsinteressen staatlicher Akteure, mit denen er sich auch auf überstaatlicher Ebene bereits in seiner Diplomarbeit mit dem Titel „Innere Sicherheit in Europa“ bereits beschäftigt hatte. Mit dem Vertrag von Amsterdam wurde 1997 der Grundstein für das politische Konstrukt des „Raums der Freiheit, der Sicherheit und des Rechts“ gelegt. Diese Formulierung wurde nun auch in die Präambel der Menschenrechtscharta der EU eingeführt – und entspreche sinngemäß dem in Grundgesetz verbrieften Grundrecht auf körperliche und geistige Unversehrtheit für jeden Menschen in seinem Geltungsbereich.
In den darauffolgenden Zeitraum fallen die zahlreichen neuen Sicherheitsgesetze, die seit 9/11 neu eingeführt wurden und mit denen u.a. neue Möglichkeiten der Kontrolle und der Datenabschöpfung auch im Internet durchgesetzt werden sollten. Sander beschäftigt sich zunächst mit der Frage, wie Sicherheitsgesetze entstehen. Die Akteure sicherten sich durch Forderungen nach Sicherheitsgesetzen ab. Ereignisse wie 9/11 oder vorher im Dunstkreis der RAF u.Ä. wurden dazu genutzt, mit einigem Aktionismus vorbereitete Gesetze durchzusetzen; dabei können diese Sicherheitsgesetze im totalen Widerspruch zu unseren Grundrechten stehen. Eine wesentliche Motivation, möglichst viele Daten ermitteln zu können, sei dabei zentral. In einem von Sander geführten Interview im Rahmen seiner wissenschaftlichen Arbeit mit einem Polizisten von Europol äußerte sich dieser offen: „Wir von der Polizei werden nie aufhören, noch mehr Daten zu fordern.“
Der deutsche *Bundes InnM Friedrich versuchte diese Prioritätenverschiebung (hin zu mehr Handlungsbefugnissen der Sicherheitsbehörden hinsichtlich umfassenderer Datennutzung) werbewirksamer als „Supergrundrecht auf Sicherheit“ anzupreisen.
Vor dem Hintergrund dieser verstärkt bemühten Begründungsfiguren wurden auf EU-Ebene in den letzten zehn Jahren 239 *Anti-Ter-Maßnahmen eingeführt, darunter 88 bindende *Anti-Ter-Gesetze. Auf diese Weise erhielt der „Raum der Freiheit, der Sicherheit und des Rechts“ seine aktuelle Gestalt.
Ein weiterer Trend bei der Art des Zugriffs auf bislang schwerer zugängliche Daten verstärkte sich zunehmend: Nicht der Staat allein sammelt das Gros der Daten, sondern greift auf **von Unternehmen gesammelte Daten** zurück. So wurde im Zuge der **Vorratsdatenspeicherung** insbesondere auf Reisedaten zugegriffen, die von den Fluggesellschaften erhoben werden sollten. Die Snowden-Dokumente verdeutlichten der Öffentlichkeit diese Vorgehensweise, von Unternehmen gesammelte Daten massenweise abzuschöpfen. Bei den über Glasfaserkabeln ausgespähten Daten sei etwa noch unklar, ob der über den Frankfurter Internetknotenpunkt DeCix laufende Datenverkehr möglicherweise vollständig angezapft worden sei: Offiziell seien nur 20% dieses Internetknotens tatsächlich ausgelastet – gleichzeitig wurde bekannt, dass 20% der über diesen Knoten laufenden Kommunikation abgehört

werde. Eine immer umfassendere Abschöpfung der Kommunikation sei anzunehmen. *GeDi-e agierten jenseits von Grundrechten und jenseits des gesellschaftlichen Konsenses – es bestehe die Gefahr, dass sie einen Staat im Staat bilden würden, wenn sie sich nicht an gesellschaftliche Vorgaben halten. Es habe sich wiederholt herausgestellt, dass die **Kontrollmechanismen** vollkommen versagt haben bzw. bei der *GeDi-kontrolle nicht effektiv sind.
So habe das Parlamentarische Kontrollgremium des Deutschen Bundestages keine Durchsuchungsrechte und durften *GeDi-mitarbeiter nur befragen. Die hieraus resultierenden Forderungen lauteten hier, das Personal im Mitarbeiterstab des PKGr aufzustocken, um überhaupt eine effektive Arbeit leisten zu können.
Sander stellt zudem in Frage, ob die Strukturen der *GeDi-organisation in der BRD angemessen seien, da trotz 16 Landeszentralen des *VerfSch-es die Aufklärung der NSU-Morde nicht geleistet wurde.
Auch die Vorratsdatenspeicherung von Kommunikationsdaten jedes Menschen anlasslos und verdachtsunabhängig verstoße grundlegend gegen das einschlägige Urteil des Bundesverfassungsgerichts, das das informationelle Selbstbestimmungsrecht begründete.
Selbst die Gewinnung ausschließlich der Metadaten der Telekommunikation verletzten etwa den schützenswerten Bereich des Datenaustausches mit Geheimnisträgern wie Rechtsanwälten, Geistlichen, Ärzten, etc. .. . Allein aus der Quantität der Kommunikation zu bestimmten Uhrzeiten mit spezifischen Personen, seien Rückschlüsse auf juristische oder gesundheitliche Probleme zu ziehen.
Die Vorratsdatenspeicherung von Fluggastdaten werde in den USA seit den 60er Jahren unter dem Schlagwort „Passenger name record“ (PNR) recht detailliert betrieben: Bis zu 60 Einzeldaten für eine einzelne Person bei einem einzigen Flug werden hier erhoben; zudem bietet ein Freifeld Gelegenheit, hinweisgebende Zusatzinformationen wie die besondere Gestaltung eines aufgeschlagenen Buchdeckels der Fluglektüre zu beschreiben oder den mitgebrachten Apfel nicht unerwähnt zu lassen. Ein Überflug des betroffenen Passagiers über den US-Luftraum bietet einen rechtlich hinreichenden Anlass, diese PNR-Daten zu erheben, an die zuständigen US-Behörden weiterzugeben, von denen sie 15 Jahre gespeichert werden. Dort können sie für weitere Fahndungen verwendet werden oder im Verdachtsfall sogar zu „No-Flight-Orders“ führen, dies bedeutet ein langjähriges Verbot für Verdächtige, ein Flugzeug, das den Luftraum der USA passiert, auch nur zu betreten.
Derzeit wird im EU-Parlament diskutiert, ob auch in der EU eine zur PNR („passenger name record“) analoge verpflichtende Datenabfrage für eine Datenbank zu EU-Flügen mit einer Speicherdauer von 5 Jahren eingeführt werden soll. Ziel dabei soll sein, bisher unbekannte Verdächtige zu finden: Mittels Data-Mining und Profiling können so Terrorverdächtige kreiert werden.
Der europäische Rat steht diesem Vorhaben sehr positiv gegenüber; dabei ist Großbritannien die treibende Kraft für die Einführung eines „passenger name record“ und fordert, diese Datensammlung nicht nur für innereuropäische Flüge anzuwenden, sondern auch auf Schiffe und Autos auszuweiten.
Trotz der Snowden-Enthüllungen werden weitere und noch tiefergreifende Sicherheitsgesetze gefordert.
Auch öffentlich zugängliche Daten sollen mittels Data-Mining-Projekten durchsucht werden mit dem Ziel, „abnormales Verhalten“ automatisch zu erkennen. So werden als Datenquellen Videoüberwachungsaufnahmen und Einträge in Internetforen herangezogen, gleichzeitig kann man über Fotos **Gesichtserkennungssoftware** (mit teilweise recht hoher Trefferwahrscheinlichkeit bzw. richtiger Zuordnungsquote) laufen lassen, um zudem Personen relativ sicher identifizieren zu können.
Auf Basis dieses Datenmaterials soll **abnormales Verhalten** nun **automatisiert eingestuft** und erkannt werden – hierzu kann bereits das (über eine relativ kurze Zeitspanne hinausgehende) Herumstehen auf einem öffentlichen Platz gehören. Dieses Beispiel verdeutlicht bereits, dass es enorm viele

Möglichkeiten gibt, **fehlerhafte Aussagen aus Datensammlungen zu ziehen** oder auch **fehlerhafte Datensätze zu produzieren**.

Auch die verstärkt herangezogenen von Unternehmen gesammelten Daten können fehlerhaft sein: wie beispielsweise eine falsch zugeordnete Sitzplatznummer, eventuell auch bedingt durch einen Sitzplatzwechsel. Tatsächlich werden offensichtlich **unschuldige Personen verdächtigt** – wie etwa ein dreijähriges Kind (wohl aufgrund eines PNP-Datensatzes) – mit gravierenden Folgen: Ist eine Person einmal als verdächtig eingestuft worden, so steht das Verbot im Raum, den US-Luftraum auch nur passieren zu dürfen.
Eine weitere Fehlerquelle kann in den Algorithmen liegen, die die teils riesigen, möglicherweise durch Verknüpfungen vergrößerten Datensätze nach Mustern durchpflügen; zudem sind diese **Algorithmen** mittlerweile „**selbstlernend**“. Hier müsse die Minimalforderung lauten, dass zur Generierung eines Terrorverdachts nicht der Algorithmus allein ausschlaggebend ist, sondern immer auch zusätzlich von einem Menschen am Einzelfall überprüft werden müsse.
Nicht nur die Fehlerquoten bei der Verdächtigung Unschuldiger aufgrund minimaler Hinweise ist problematisch – grundsätzlich äußerst fragwürdig ist die **Umkehr der rechtsstaatlich begründeten Unschuldsvermutung**, indem Verdächtigungen kreiert werden aufgrund relativ willkürlicher, nicht beweiskräftiger Merkmale und Anhaltspunkte im durchstöberten Datensatz. Als in der BRD präsentes Beispiel führt Sander eine Riege zu Unrecht dauerhaft unter Terrorverdacht geratener Soziologen an, unter ihnen André Holm, dessen absurder Fall von Bürgerrechtlern bekannt gemacht wurde.
Zunehmend mehr Datenarten liegen in wachsenden Mengen in digitalisierter Form vor, darunter etwa von google gesammelte E-Mail-Daten bis hin zu Gesundheitsdaten wie Rezeptdaten bzw. Verschreibungen für Krankheitsfälle, die bereits für etwa 1,5 Cent bis 5 Cent auf dem Datenmarkt zu haben sind.

Eine Ursache für den **praktisch lückenhaften Datenschutz** seien die bewusst **ausgewählten Standorte**, an denen die Server platziert werden, über die die meist international weitergeleiteten Datenfluten laufen – wobei das ausschlaggebende Auswahlkriterium für einen Standort oft das niedrigste Datenschutzniveau eines Landes sei, wie etwa bei dem in Irland installierten facebook-Server angenommen werden kann.
Diese Unternehmen, die mit Massen datenschutzbedürftiger Daten umgehen, gingen bereits gehäuft an die Börse, so dass der Druck zur Gewinnmaximierung auf die Unternehmen bzw. Konzerne weiter massiv ansteigt. Die Frage laute, was ein Konzern wie facebook unternehmen werde - insbesondere im Umgang mit den ihm zur Verfügung stehenden Daten - wenn sein Börsenkurs anfängt zu sinken.
So gingen AOL und myspace bereits Pleite; fraglich sei dabei, wo die die von diesen Unternehmen bearbeiteten Daten verblieben seien.
Hinzu kommen Datenpannen und Datenlecks, durch die Datenmengen unvorhergesehen diffundieren können bzw. einfach abgesaugt werden können.

Gerade auch vor dem Hintergrund der besonders kritischen genannten Probleme, die man als eher unintendierte Nebenfolge des Datensammelaktionismus einstufen kann – von Datenpannen bis hin zu falschen Verdächtigungen von unbescholtenen Bürgern, die ins Visier von Ermittlungsbehörden geraten können, sollte besonders das Ausmaß der verfügbar gemachten Datenmengen und -arten nicht aus dem Blick geraten. – Gerade die Spanne der verwendeten Datentypen müsse bewusst gemacht werden, die eine Überwachung nicht nur im Internet ermöglichten, sondern sämtliche unserer Bewegungen auch im realen Raum auswertbar mache und in einer Art

„**Überwachungsgesamtrechnung**“ betrachtet werden sollten. Diese zusammentragbare Datenspanne verdeutlicht das Ausmaß der bereits möglichen Überwachungsmöglichkeiten.
Überdacht werden müsse gerade auch der **Einschüchterungseffekt** auf Personen, die eine Überwachungssituation vermuten können – hier müsse unbedingt hinterfragt werden, ob **demokratische Mitwirkungsbedingungen** nicht zu stark beeinträchtigt würden.

Nach den **239 neuen Gesetzen und Maßnahmen**, die **in der BRD** im Rahmen der Sicherheitspolitik seit den 2000er Jahren erlassen worden sind, bestehe zunehmend die Gefahr der Entwicklung eines totalen Überwachungsstaates, der übermäßig Druck zu vorauseilendem angepasstem Verhalten ausüben würde. Wenn die Angst vor **negativen Konsequenzen aus** zu erwartenden, zudem **personenspezifischen Datensammlungen** in typischen (auch gesellschaftspolitisch relevanten) Situationen realistisch erscheine, werde ein deutlicher Druck hin zu **angepasstem Verhalten** erzeugt, sich etwa mit freier Meinungsäußerung zurückzuhalten, Demonstrationen nicht zu besuchen oder auch möglicherweise keinen engeren Kontakt mit politisch interessanten, als potenziell verdächtig einstufbaren Personen zu pflegen. Wenn solche Verhaltensweisen wahrscheinlich werden, entstehe ein Sicherheitsstaat, der keine wirklich demokratischen Diskussionen unter unbelasteten Voraussetzungen mehr zulasse.
Um ein Abrücken weg von demokratischen Grundbedingungen hin zu sicherheitsstaatlich einschüchternden Handlungsbedingungen abzubremsen, sei eine **neue Datenpolitik** notwendig, die selbstverständlich auch **weitgehende Datenschutzregelungen** sichere.
Aktuell steht hier die Datenschutzreform auf EU-Ebene auf der Agenda: Im Europäischen Rat würden hier derzeit Datenschutzhandlungen blockiert, welche wohl verwässert und weiter herausgezögert werden sollen, wobei gerade auch die BRD eine maßgebliche Rolle spiele. Bei diesen anstehenden Beschlüssen zu Datenschutzregelungen auf EU-Ebene ist es wesentlich, die formale juristische Festschreibungsweise zu beachten: Unterschieden werden kann zwischen einer **Richtlinie**, die nur eine Grundlinie als Vorgabe für die Mitgliedsländer zu deren teils variabel auslegbarer Umsetzung ziehen soll – und einer **EU-Verordnung**. Eine Datenschutzverordnung muss von den Mitgliedern direkt und unmittelbar ohne weiteren eigenen Auslegungsspielraum der Mitgliedsländer umgesetzt werden. Eine Datenschutzverordnung wurde angekündigt. Eine Datenschutzreform auf EU-Ebene müsse auch **für Unternehmen und andere Akteure aus Drittländern** wie der USA vollständig anwendbar sein, ohne dass sich diese den EU-Datenschutzgesetzen entziehen könnten, indem etwa deren Server in Drittländern mit niedrigerem Datenschutzniveau platziert werde.
Als weitere Maßnahme einer neuen Datenpolitik wären deutlich sichtbare Symbole im Internet, die den jeweiligen Standard des Umgangs mit den Nutzerdaten auf einer Internetseite klar ersichtlich anzeigen, also einer Kennzeichnung dafür, was mit den eigenen Daten weiterhin passiere. Die aktuellen AGBs werden zu selten gelesen, da sie praktisch zu lang und zu kompliziert formuliert werden.
Nicht zu vernachlässigen sei auch die **datenschutzorientierte Verteilung von Forschungsförderungsgeldern**. So dürften einerseits nicht Techniken zur Internetüberwachung mit Steuergeldern unterstützt werden, umgekehrt gäbe es auf EU-Ebene nur ca. fünf bis sechs Forschungsprojekte, die sich mit den Gefahren der Überwachung im Internet etwa in diktatorischen Staaten beschäftigen. Ein großer Teil der zu Forschungszwecken ausgegebenen Gelder werde an Rüstungskonzerne vergeben, den **ersten Einsatzort zur Erprobung der neuen Technologien** bieten oft Aufgaben im Grenzschutz.

Nicht alles, was juristisch durchsetzbar sei, müsse auch umgesetzt werden – so etwa die weitgehenden Terrorgesetze.

Ein zentraler Punkt einer neuen Datenpolitik sei auch die Transparenz im Umgang mit den zugrunde gelegten Annahmen bei der Datenauswertung. **Transparenz bei automatischen Entscheidungsprozessen** (wie beispielsweise beim Schufa-Scoring) müsse dringend gegeben sein. Zunächst müssten nicht nur alle eigenen Daten eingesehen werden können, sondern insbesondere auch die **Algorithmen zur Generierung von Verdächtigen** müssten **zwingend offen gelegt** werden. Nicht zuletzt sei natürlich der Umgang mit Nichtregierungsorganisationen im Aufgabenbereich Datenschutz und informationeller Selbstbestimmung ein wichtiger Dreh- und Angelpunkt. Schließlich sei die Unterstützung von Nichtregierungsorganisationen eine die neue Datenpolitik unterstützende Maßnahme. Projektförderungen und Basisförderungen von NGOs (Non Governmental Organisations) im Aktionsbereich für informationelle Selbstbestimmungsrechte und Datenschutzpolitiken auch aus der EU seien hier genannt.
Alle diese Maßnahmen stützen eine Trendumkehr weg vom Sicherheitswahn mit den Mitteln grenzenloser Überwachung hin zur Verteidigung einer freiheitlichen Gesellschaft.

In der am Ende dieses Vortrags anschließenden Fragerunde wurde weiterhin die besonders intransparente Ausküngelung von Sicherheitsgesetzen insbesondere durch Trebi oder den Wiener Kreis thematisiert. Vorfeldorganisationen, die frühzeitig und im Vorfeld diskutierter gesetzlicher Maßnahmen bereits Netzwerke zum Datenschutz aufgebaut haben.
Über die Effektivität dieser präventiven Form der Terrorabwehr und der Vermeidung schwerer Straftaten gebe es keine statistischen Veröffentlichungen: insbesondere darüber, wie viele Datensätze gesammelt werden, wie viele Verdächtige gefunden und wie viele Schuldige ermittelt wurden.
Dass **Begründungsansätze der Ter*- oder OK-Bekämpfung für Datensammlungen künstlich kreiert sein können**, belegten bereits einfache Erfahrungswerte, so werden beispielsweise Drogen i.d.R nicht mit Passagierflugzeugen befördert, sondern per Frachtgut etc.
Sander setzt auch bei der Verhältnismäßigkeit insbesondere von dauerhaften Totalüberwachungsmaßnahmen an: Hier sollte eine Gültigkeitsbeschränkung [## des Gesetzes auf die Dauer von fünf Jahren] der Dauer auf fünf Jahre befristet werden und nach diesem Zeitraum neu diskutiert werden.

Auf eine Zuhörermeldung zur **Videoüberwachung** fragt Sander erneut nach der **Zweckmäßigkeit** des Kameraeinsatzes: Können tatsächlich Straftaten verhindert werden oder bewirkt die Kamera lediglich eine anschließende Verlagerung der Kriminalität an einen anderen Ort? Zudem stellten sich hell erleuchtete Straßen als sicherer und somit zweckmäßiger heraus als videoüberwachte Straßen. Die Grundfrage laute vor allem, ob ein Mittel verhältnismäßig und angebracht sei.
In diesem Zusammenhang sei auch die Frage wesentlich, **welche Technik eingesetzt werde** wie etwa Gesichtserkennung. Grundsätzlich **nicht** mehr **verhältnismäßig** sei eine flächendeckende Überwachung aller Menschen in Europa – auch wenn sie einen Terroranschlag verhindern könne.

Für den US-Kongress habe eine Kommission zwei Jahre lang die Frage geprüft, **wie effektiv die umfangreiche Datensammlung** hinsichtlich des Ziels der Terrorvermeidung sei; das Resultat dieser Untersuchung war, dass keine (nennbaren) Terroranschläge verhindert wurden. Die Kommissionstätigkeit wurde hiernach eingestellt.
Eine weitere Frage zielte darauf ab, ob ein Bürger jedes Mal informiert werden solle, wenn seine Daten abgesaugt werden. Sander plädierte an dieser Stelle für eine **Opt-In-Möglichkeit jeden Bürgers**, die bedeutet, dass die Weitergabe seiner eigenen Daten zuerst und zwingend von seiner eigenen Zustimmung abhängig sein muss.

Eine weitere Frage zielte auf die Rolle privater Unternehmen ab. Hier wurde zunächst auf die zuletzt zahlreichen Aufkäufe kleinerer Firmen mit spezifischen funktionalen Spezialisierungen (im digitalen Bereich) durch große US-Internetfirmen verwiesen, insbesondere facebook und apple hatten zuletzt zahlreiche kleine Firmen zu immens hohen Preisen aufgekauft. Sander sah diese Entwicklung als weniger relevant an als die Tatsache, dass die **großen Internet-relevanten Konzerne börsennotiert** sind. Diese Internetfirmen leben von der Ansammlung der Daten der Nutzer, so Sander und verwies auf die bereits mit facebook gemachte Erfahrung, dass Nutzer-Daten selbst nach der account-Löschung auf Wunsch des betroffenen Nutzers weiterhin auf facebook-Servern gespeichert waren. Vor dem Hintergrund dieser Erfahrungen sei umso dringlicher, dass **Sanktionen zur Abmahnung von rechtsbrechenden Unternehmen** möglich sein müssen.
Die noch **unterschiedlichen bestehenden Rechtsstandards gerade zwischen den USA und der BRD** stellten hierbei eine weitere Hürde dar. So darf in der BRD das Unternehmen A, das das Unternehmen B kauft, nicht automatisch alle Daten von Unternehmen B nutzen. In den USA hingegen darf ein aufkaufendes Unternehmen A das.

3) Ingo Mersmann, Geschäftsführer: „Die Sicherheitsinteressen des Staates angesichts von Terrorabwehr und Schwerkriminalität – was ist akzeptierbar?“

Als nächster Redner eröffnete Ingo Mersmann als Geschäftsführer des Instituts für Spionage GmbH neue Perspektiven in die Welt der Spionage.
Angekündigt wurde Mersmann als Kunsthändler, der der Frage nachgehen wollte, welche Sicherheitsinteressen des Staates angesichts von Terrorabwehr und Schwerkriminalität akzeptierbar seien.
Mersmann gab überraschend weitergehende Einblicke in seine Erfahrungshintergründe: Er selbst habe über 28 Jahre unter anderem Namen für einen Nachrichtendienst gearbeitet. Der erste Kontakt war bereits hergestellt, als ihn auf Anfrage hin eröffnet wurde, dass das künstlerische Institut an einer Universität, an der er gearbeitet habe, nicht von der Universität selbst, sondern vom *BN finanziert wurde. Man war an seiner Mitarbeit für den Nachrichtendienst interessiert und er willigte ein. Heute verlaufe der Einstieg in den BND weniger konspirativ: „Heute bewirbt man sich selbst beim BMI.“ Erste Kontakte können in Veranstaltungen hergestellt werden, die etwa nur von Anwendungsinformatikern besucht werden.
Ein typischer Auftrag für den *BN könne sein, vor Ort zu ermitteln, wie Drogen von Südamerika in die BRD geschmuggelt werden. Bei dieser klassischen Form der „Human Intelligence“, begeben sich ##**Informanden* hinein in die interessierenden Szenen.
Hier könnten typische Begrifflichkeiten der Szene abgeschöpft werden, um damit anschließend digital nach solchen Begriffen zu suchen. Der *BN dürfe nur im Ausland arbeiten, während der *BV zwar im Inneren arbeite, aber für die benötigten Technologien kaum Geld habe, und diese somit nur vom *BN zur Verfügung gestellt werden können, die Technologien werden zudem auch dort entwickelt.
Die bereits angesprochene „Human Intelligence“ ist eine klassische *GeD-Aufgabe, mittels der Kontakte zu Menschen hergestellt werden, zu beobachten, wie eine Zielperson in den letzten Monaten und Jahren gelebt habe, und deren Schwachstellen zu erkennen; (## diese Person dann möglicherweise anzuwerben).
*BN startet wie bereits ausgeführt mit Human Intelligence, um anschließend Signal Intelligence einzuführen. Anders sei es bei der *NA, dort werden Daten vom Dienst eventuell auch privaten Unternehmen zur Verfügung gestellt, um damit auch etwas Geld zu verdienen, dies könne eine Summe von 90 Milliarden $ pro Jahr einbringen.
In den unter internationalen *GeDi durchgeführten Umfragen werde der *BN immer wieder als bester Dienst eingestuft, da er sehr gut und sehr effektiv arbeite und zudem eine sehr gute Ausbildung biete. Die Ausbildung beim *BN umfasse sechs Jahre, davon zwei Jahre Grundausbildung und vier Jahre Spezialausbildung. Anschließend werden zunächst Human Intelligence-Aufgaben durchgeführt oder schriftliche Quellen wie Zeitungen und Dissertationen ausgewertet.
Beispielsweise ergab sich aus der Analyse einer solchen Doktorarbeit, dass der *Ir vor 15 Jahren bereits auf einem wissenschaftlichen Stand war, der zehn Jahre weiter war als zuvor angenommen. Der *M wird mit der Tötung der führenden *ir-ischen *Atwissenschaftler in Zusammenhang gebracht; während der *BN solche Tötungen nicht durchgeführt hätte.
Die Aufgaben des *BN wie des *BK sei es, *Terverdächtige zu ermitteln, zu erwischen und möglicherweise außer Landes zu verweisen.
*GeDi seien strikte Gegner **öffentlicher Gerichtsverhandlungen**, da so die Fehler der *Terverdächtigen offen gelegt würden, die dazu geführt hätten, sie dringender zu verdächtigen. Um also die Tätigkeit der

*GeDi nicht in das grelle Licht der Öffentlichkeit geraten zu lassen und Mitschriften potenzieller Mitstreiter von Verdächtigen in Gerichtssälen zu vermeiden, die zu Lerneffekten und zur besseren Tarnung zukünftiger Täter führen können, versuchen die *GeDi derartige Gerichtsprozesse zu vermeiden. Eine andere Art des Umgangs mit *Terverdächtigen sei der „geheime Kanzlerentscheid", also Liquidationen von *Terverdächtigen, die vom Kanzler/der Kanzlerin getroffen werden dürften. Bei der allwöchentlichen Lagebesprechung im Kanzleramt zwischen Kanzler und Kanzleramtsminister können solche geheimen Entscheide fallen, die nur als mündliche Entscheidungen getroffen werden, von denen es keine Protokolle gebe. Zur Ausführung könne Zugriff auf den *BN genommen werden, um derartige Tötungen zu erledigen.
Seit 1990 hätten sich einige Vorgehensweisen in den *GeDi verändert. So mussten vor 1990 im Ausland tätige GeDi-mitarbeiter nach einer möglichen Enttarnung noch ca. ein dreiviertel Jahr bis eineinhalb Jahre ausharren bis zu ihrer Rückkehr. Mittlerweile sei eine Liquidation von enttarnten *GeDlern im Ausland in den Bereich des Möglichen gerückt, wenn er den Dienst in Gefahr bringe.
Auch für das private Umfeld gebe es relevante Regelveränderungen: Für normale *GeDtätige werden doppelte Identitäten verwendet, die bei Einsätzen verwendet werden, hier wurden bislang selbst Ehepartner nicht darüber informiert, dass ihr Partner Monate lang im Ausland für den *BN tätig war. Seit vier Jahren darf der Lebenspartner wegen der langen, teils kaum erklärbaren Abwesenheitszeiten über eine Agententätigkeit informiert werden.
Auch zum Thema Whistleblower-Enthüllungen äußerte sich Mersmann : Diese werden grundsätzlich nicht kommentiert. Zukünftig werde der *BN aber offener und transparenter – ähnlich wie der *MI und *GC: Es werde Pressekonferenzen und Führungen durch das neue *BN-Gebäude in Berlin geben.

Im Zusammenhang mit Drohneneinsätzen erwähnte Mersmann ein zur Personenidentifizierung verwendetes Programm, das anhand von Bewegungsapparat und Motorik eines Menschen mit etwa 72%iger Wahrscheinlichkeit eine Zielperson identifizieren könne. Bei den Drohneneinsätzen liefe nicht nur die Kommunikation, sondern letztendlich auch der Abschuss satellitengesteuert.
Er verwies weiterhin auf die extreme Realitätsnähe des 1998 produzierten US-Spielfilms „Staatsfeind Nr. 1" mit Will Smith, in dem auch technische Erhebungen von Aufenthaltsdaten dargestellt wurden.
Auch in der DDR verwendete Aufklärungstechnologien wurden in einem Rückblick erwähnt: So wurden damals Infrarotanlagen in Trabis verwendet, um Treffen von Personen auszukundschaften, wobei vorteilhaft war, dass das Infrarot die Plastik-Karosse des Trabis durchdringen konnte.

Zur *NA-Affäre merkte Mersmann an, dass es vollkommen normal sei, „bei den anderen mal reinzuschauen."
Er sprach sich für eine weitere Ausdehnung der Vorratsdatenspeicherung aus, es gebe ja bereits kaum noch ungenutzte Daten. Von den Handy-Fotos, die beim *BN landen, können 70% der fotografierten Personen identifiziert werden. Die notwendigen Technologien gebe es alle schon, die für eine umfassende Datensammlung genutzt werden können. Die Daten aller Bundesbürger passen in ein kleines Einfamilienhäuschen. Zudem gebe es sowieso keine 100%ige Sicherheit der Daten, auch nicht über Maßnahmen wie Verschlüsselung etc..

Auf die Frage, wie bei der Möglichkeit vorgegangen werde, wenn private Hacker Daten stehlen, führte Mersmann aus, dass der *BN Kontakte in den digitalen Ausschuss des Deutschen Bundestages habe sowie zum Parlamentarischen Kontrollgremium. Es gäbe Ausschüsse, in denen der *BN mit drin hänge, um dafür zu sorgen, dass Daten geschützt werden können.

Zum Beispiel Maut-Technologie erläuterte Mersmann, dies sei eine rein politisch-wirtschaftliche Entscheidung, der *BV brauche die Maut-Prüfung nicht.

Im weiteren Zusammenhang erklärte Mersmann, die Dienste könnten heute Daten sammeln, wo sie wollten, sie preschten aber nicht überall vor, um neue Datensammlungstechnologien und –methoden durchzusetzen, da dies nicht nötig sei.

Zu Snowden merkte Mersmann an, dass es gut sei, dass die Öffentlichkeit über die Art der Datensammlung informiert werde und der Bürger weiß, wie so etwas funktioniere. Es sei aber nicht gut, dass Snowden als Mitarbeiter seinen Richtlinien nicht gefolgt sei.

4.) Olaf Tenti, Gesellschaft für Datenschutz und Informationssicherheit, Hagen: „Datenspuren gibt es nicht nur im Internet – wie können Bürgerinnen und Bürger ihre Privatsphäre sichern?“

Olaf Tenti von der Gesellschaft für Datenschutz und Informationssicherheit in Hagen beschrieb ein Spektrum von Alltagstechnologien, über die große Mengen personenbezogener Daten gesammelt werden können. In seinem Vortrag mit dem Titel „Datenspuren gibt es nicht nur im Internet – wie können Bürger und Bürgerinnen ihre Privatsphäre sichern?“ befasste sich Tenti auch mit weniger breit bekannten Möglichkeiten technischer Datenabschöpfung und einigen Möglichkeiten, diese zu begrenzen.
Zuerst stellte Tenti exemplarisch eine vielseitige Reihe von **Interessen am Datenhandel** in verschiedenen gesellschaftlichen Bereichen zusammen: Im ökonomischen Bereich interessierten sich Kaufleute dafür, wer was von wo kaufe, wie man Werbung effektiver versenden und in ihrer Wirkweise optimieren könnte. Es ginge nicht nur um das Verkaufen von Waren, sondern auch um den unmittelbaren Handel mit Daten (etwa von Payback-Daten), aber auch um Wirtschaftsspionage. Mit dem Schlagwort „**Pre-Fetching**“ wird der Hunger von Unternehmen beschrieben, Kundeninteressen so frühzeitig wie möglich auszukundschaften: So stehe es etwa im Interesse Amazons „zu wissen, was Sie kaufen, bevor Sie etwas kaufen“. Zukünftig könne die technische Möglichkeit per Drohne genutzt werden, Waren auszufragen, denen ein RFID-Chip anhaftet.
Behörden erheben zunehmend Daten etwa zu Fahndungszwecken – z.B. bei Steuerdelikten, um Täter zu finden; mittlerweile wurde beispielsweise veröffentlicht, dass bei einer Geschwindigkeitsübertretung ein Raser durch ein facebook-Foto identifiziert wurde. Auch um Sanktionslisten zu erstellen, wobei die Kriterien, um auf eine solche Sanktionsliste zu gelangen, nicht transparent sein müssen.
Neben derartigen Fahndungszwecken verkaufen auch staatliche Behörden Bürgerdaten – so etwa Einwohnermeldedaten oder auch Kfz-Zulassungsdaten.
Natürlich haben auch Kriminelle Interesse an personenbezogenen Daten. Bei der Vorbereitung von Straftaten wie Einbrüchen können etwa über facebook Abwesenheitszeiten erschlossen werden. Zum Bankbetrug, für einen Identitätsdiebstahl insbesondere zur Kreditkartenfälschung werden Name, Geburtsdatum, Kreditkartennummer und Prüfsumme der Kreditkarte benötigt. Ein Datensatzwert auf dem Schwarzmarkt betrage zwischen 10 Cent und bis zu einem Dollar, wenn die Prüffrage (wie beispielsweise der Geburtsname der Mutter) mit enthalten sei.
Im Bereich Mobbing im Internet gäbe es mittlerweile Dienstleister über Drittanbieter für etwa 150 €. Ebenso werden Daten für die Durchführung von Straftaten wie etwa Kreditkartenfälschung benutzt.

Zur Beantwortung der Frage, warum wir schon alle gläsern sind, zählt Tenti ein „**Big Data Roundabout**“ vor: **Datenquellen** seien Krankenkassendaten inklusive sensibler Gesundheitsdaten, Gehaltsabrechnungen, Bankdaten, Stundennachweise für Arbeitsaufgaben, Steuerdaten, Internetsurfen, Handyrechnungen und Verbindungsdaten, Handynutzungen, aus denen Bewegungsprofile erstellt werden können, Apps, in deren AGBs das Lesen, Schreiben und Löschen auf dem betroffenen Gerät bestätigt werden sollen, allgegenwärtige Sicherheitslücken auf Handys, durch

die es leicht gelingt, Handys (offenbar auch bevorzugt auf solchen junger Frauen) zu kapern, sowie Kreditkartendaten.
Über benutzte Dienste können ebenfalls Daten weitergeleitet werden, so über facebook, über smartmeter zur Messung spezifischer Verbrauchsdaten im Haushalt, RFID-Chips, Payback und Co., Yellow Dots, das Navi im Auto, E-Mails (wie die Snowden-Enthüllungen verdeutlichen, werden etwa von der *NA mehrere Millionen E-Mails im Jahr durchleuchtet sowie Mitschnitte gespeichert. Hinzu kommen die Videoüberwachungen und Kamerainstallationen wie 24-Stunden-Videoüberwachungen an EC-Kartenautomaten, in Bussen, an Bushaltestellen, Bahnhöfen, Läden, neuerdings auch in Krankenwägen (!), auf öffentlichen Plätzen, in Shopping Malls. – In Großbritannien sei eine komplette Videoüberwachung möglich (die das öffentliche Leben weitgehend abdeckt).

Solche Daten können zu verschiedenen Zwecken gefragt sein: So funktionieren Staufinderfunktionen eines Navis, indem an dessen Heimstation Ort und Geschwindigkeit weitergeleitet werden. Bei etwa 50 Meldungen von 50 Kunden mit nahezu keiner Geschwindigkeit kann auf einen Stau geschlossen werden. Auf Basis der gleichen Daten (Ort und Geschwindigkeit) könne auf Geschwindigkeitsüberschreitungen geschlossen werden, für die sich wiederum die Polizei interessiere.

Auch die **soziale und politische Beurteilung** (einmal herausgegebener Daten) **könne sich** im historischen Verlauf leicht **wandeln**: So gab es in den 1920er Jahren bereits viele Homosexuelle, die dies offen zeigten – in den 1930er Jahren wurde dies bereits von den Nazis als Grund herangezogen, in KZs eingewiesen zu werden. Heute werden derartige Daten als irrelevant betrachtet, es sei aber nie sicher absehbar, wie lange welche Daten wirklich niemanden interessieren.

Andere **Daten** können durch technische Geräte plötzlich **auslesbar gemacht** werden: So RFID-tacks durch „Radio Frequency Identifiers“, wodurch etwa Bezahlkarten ausgelesen werden könnten. Auch RFID-tacks an Kleidung sind aus fünf cm Entfernung auslesbar und geben Angaben über Hersteller, Größe, Alter des Modells sowie die Farbcodierung preis.
Mit dem **Smartmeter** wird der Stromverbrauch zu jeder Uhrzeit ablesbar, das Verbrauchsprofil lasse je nach ausgewerteter Dauer bis zu etwa 15 Minuten auf Hersteller und Verbrauch eines Elektrogeräts schließen, welche Elektrogeräte benutzt werden, wie viele Bewohner im Haus seien und sogar das Fernsehprogramm, das gesehen wird, lassen sich identifizieren. Über wiederholte Gebrauchsparameter zu bestimmten Uhrzeiten lassen sich Gewohnheiten ablesen.

Die Datenschutzzuständigkeiten können hingegen offenbar mitunter auch vom Unternehmen ausgesucht werden: facebook habe eine „funny stuff data protection“; für facebook ist nach eigenen Angaben des Unternehmens eine Datenschutzstelle zuständig, welche den Milliarden-Konzern kontrollieren solle, die in einem bereits äußerlich eher bescheiden aussehendem Gebäude zu finden ist. Einen facebook-account könne man bereits nur per E-Mail-Adresse des vermeintlichen facebook-Nutzers eröffnen. Eine facebook-Einnahmequelle baue darauf auf, zu wissen, wann der Nutzer wie lange mit wem kommuniziert habe.

Die **Sensibilität von personenbezogenen Daten** lässt sich noch einmal anhand der Menge der Informationen veranschaulichen, die zur Ermittlung der Kreditwürdigkeit einer Person notwendig ist: Hier reichen der Name, Wohnort, Straße und Geburtsdatum für eine Online-Kreditanfrage aus. Mit diesen Minimaldaten könne über diesen Weg letztendlich die Kreditwürdigkeit bei der Schufa

verschlechtert werden. **Die Summe der gesammelten Daten vergrößere die Möglichkeiten des Missbrauchs**.

Zusammenfassend lasse sich feststellen, dass der gläserne Bürger bereits Realität sei. Die freiwillige Datenherausgabe vergrößere aber auch die potenzielle Angriffsfläche. Der alleinige Ruf nach staatlichem Schutz reiche nicht aus.
Vor dem Hintergrund moderner technischer Möglichkeiten werden die Möglichkeiten des Datenmissbrauchs ebenfalls erheblich vereinfacht: So könne heute jeder ohne technischen Aufwand eine E-Mail in jedermanns Namen versenden.
Letztendlich gebe es keine belanglosen Daten mehr: Alles kann ausgewertet werden, **Daten** können **vernetzt** und **verkettet** werden. **Empfehlenswert** wäre hier das **gesetzliche Verbot einer Profilbildung**.
Unternehmen können bislang recht **gut Datenschutzgesetzen ausweichen**: Wenn sich die Datenschutzstandards in Irland verbesserten, dann würde die Datenverarbeitung vermutlich nach Burundi verlegt werden.

Nach Abschluss dieses vierten Vortrags des ersten Tages wurden noch einmal einige wesentliche Punkte zusammengetragen:
Datensparsamkeit reiche angesichts der vielfältigen technischen Möglichkeiten der Einsehbarkeit, Abrufbarkeit und Speicherung von Daten kaum aus.
Eine **Waffengleichheit** der als Dateneigner betroffenen Bürger und den zahlreichen Unternehmern, Dienstleistungsanbietern und Institutionen, die die personenbezogenen Daten verarbeiten bzw. durch technische Möglichkeiten Zugriff hierauf erlangen, sei nicht gegeben.
Den positiven Aspekten der Netznutzung, den neuen über Internet beziehbaren Produkte und Dienstleistungen stehen die Gefahren des Machtmissbrauchs gegenüber (durch über das Internet beziehbare Daten und Sicherheitslücken in der Programmierung sowie Angriffe über das Internet).
Die **Rechtssicherheit** des Bürgers wurde seit Anfang der 80er Jahre zwar eingefordert und diskutiert, bestehe aber aktuell unter diesen technischen Gegebenheiten nicht – obwohl das Internet mittlerweile weitgehend im beruflichen und privaten Alltag unverzichtbar geworden ist.
Mit dem Internet werden neue Datenmengen und Möglichkeiten der **Verfügbarkeit von Daten** geschaffen, personenbezogene Daten aus unterschiedlichen Kontexten ließen sich miteinander verknüpfen und lassen weitgehende Schlussfolgerungen auf eine interessierende Person zu – so dass Dritte mitunter größere Einblicke in das „**Profil**“, die persönliche Lebensführung und –bedingungen, auch Motivationen erhalten können und daraus interessierende **Scorings** berechnen können als dem Nutzer bewusst sei.

Hierauf folgten nach einige Zuhörermeldungen zu Tentis Vortrag.
Eine Zuhörerfrage richtete sich auf zunehmend über das Internet geleitete Daten aus dem Gesundheitswesen. Hier solle die ISO-Norm 80.000 [oder 8000] die Sicherheit im medizinischen Umfeld sichern. Im Gesundheitswesen gebe es eine neue Entwicklung hin zur „**Telemedizin**“, in der Röntgenbilder etwa auch von entfernt sitzenden Medizinern in den USA hergestellt werden können. Selbst Teleoperationen sollen über Entfernungen über das Internet durchgeführt werden können, der hierfür bereit gestellte sichere Datenkanal sei allerdings technologischer Unsinn.
Aber auch bekanntere und verbreitetere Datenverwendungen durch Krankenkassen wurden angesprochen: So gebe es etwa Gesundheitsrabatte u.a. aufgrund der Anzahl der Fitnessstudiobesuche,

bei einem Krankenkassenwechsel werde das Profil von der alten Krankenkasse mit übertragen, wobei das Gesundheitsprofil offenkundig zu den sensiblen Daten gehöre.

Grundsätzlich gebe es zwei sich gegenüberstehende Ansprüche im Umgang mit Daten, so Tenti: Dem Bürgerinteresse nach Sicherheit der Daten stehen die Interessen insbesondere der Datenverarbeiter gegenüber, die Daten praktisch, billig und schnell verarbeiten und nutzen zu können sowie wiederholt und dauerhaft verfügbar zu halten. Bei dieser Interessenabwägung gebe es die relevanten Randbedingungen und Einflussfaktoren in der Datenverarbeitung von Geld, Personal und Zeit: Je mehr dieser Ressourcen zur Verfügung stehen, desto besser sind die Bedingungen, den sich gegenüberstehenden Ansprüchen möglichst weit entgegenkommen zu können.

Grundsätzlich sollte sich der Nutzer bewusst machen, dass kostenlose oder –günstige technische Dienstleistungen wie etwa Apps letztendlich von Nutzern mit Informationen bzw. Daten bezahlt werden, die Geldwert haben. So werde beispielsweise bei jedem Verkauf eines personenbezogenen Paybackdatensatzes an einen interessierten Weiterverwender je ca. 40€ verdient.

5.) Prof. Dr. Walter Roth von der Fachhochschule Südwestfalen, Fachbereich Informatik: „Die Nutzung von Clouds nimmt zu – was bedeutet das für meine Datensouveränität?“

Prof. Dr. Walter Roth von der Fachhochschule Südwestfalen in Iserlohn, aus dem Fachbereich der Angewandten Informatik führte in die technischen und rechtlichen Aspekte der **Cloud-Nutzung** ein, natürlich mit Fokus auf die Datensouveränität des Users.
Zunächst stellte Prof. Roth den technischen Nutzen und bekannte Anbieter von Cloud-Diensten vor, befasste sich mit üblichen Nutzungsweisen und Geschäftsmodellen sowie weitergehenden rechtlichen Hintergründen hierzu, die oft erst auf den zweiten Blick ersichtlich werden. Schließlich sprach er auch Sicherheitslücken und erste Maßnahmen zur Erhöhung der Datensicherheit an.
Einführend wurden die verschiedenen Eckdaten der technischen Leistungsfähigkeit von Cloud-Diensten vorgestellt wie Speicherplatz, Rechenkapazität, Netzwerkkapazität und Software, die über Netzwerke zur Verfügung gestellt werden. Der Nutzer verwende die Dienste und brauche sich nicht um die Bereitstellung der Hard- und Softwarekomponenten zu kümmern; während der Anbieter bestimme, wo und mit welcher Hard- und Software die Daten des Nutzers verarbeitet werden.
Prof. Roth stellte die Namen der bekanntesten Anbieter von Cloud-Diensten und deren Produkte vor wie etwa Drop Box, Deutsche Telekom, Cloud Dienst, Google Drive, Microsoft Sky Drive (OneDrive), IDrive und Wuala. Danach befasst er sich näher mit dem Begriff der Datensouveränität, für die absehbare Konsequenzen durch die Cloud-Dienst-Nutzung umrissen werden sollen. Dazu gehöre die zentrale Frage danach, wozu meine Daten verwendet werden, wann und ob meine Daten vernichtet werden, wer meine Daten erhält und viele mehr.
Die Cloud-Anbieter können mit folgenden Maßnahmen werben, die die Datensicherheit der Nutzer erhöhen sollen: Der Cloudanbieter habe gute Möglichkeiten, die Sicherheit der Daten gegen Verlust zu erhöhen; der Zugriff Unbefugter werde durch Authentifizierung des Benutzers verhindert; Verschlüsselung auf dem Übertragungsweg verhindere das Mitschneiden der Kommunikation durch Unbefugte.

Zur genaueren Beleuchtung der Datenverarbeitungsmodalitäten einiger der bekanntesten Cloud-Dienste stellte Prof. Roth einige Auszüge aus deren **Allgemeinen Geschäftsbedingungen** (AGB) vor. In den AGB der OneDrive Cloud von Microsoft finden sich in äußerst kleingedruckter Schreibweise u.a. folgende Passagen:

- „Die Dienste umfassen möglicherweise die Anzeige personalisierter Dienste und Werbung.“
- „werden gelegentlich Daten anderen von Microsoft beauftragten Unternehmen übertragen“
- „persönliche Daten können in den USA sowie in [## sinngemäß] jedem anderen Land gespeichert und verarbeitet werden“

Auch **internationale Abkommen** sind natürlich relevant für die auf Servern in anderen Ländern wie den USA verarbeiteten Daten:
Das **Save-Harbour-Abkommen** gießt die Entscheidung der EU-Kommission in eine rechtlich verbindliche Form, die es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln. Die genaueren Bestimmungen sind im Internet einsehbar.
Nach den Snowden-Enthüllungen wurden Regelungen dieser Abkommen ein wenig präziser formuliert.
Weitere Datenschutzbestimmungen der USA beeinflussen die Datensouveränität europäischer Bürger:

Insbesondere einschlägige Sicherheitsgesetzgebungen der USA betreffen die oft über die in den USA stehenden Server geleiteten und verarbeiteten Daten auch europäischer Bürger.
Näher betrachtet wurden hierzu drei maßgebliche US-Sicherheitsgesetze:

1.) Der **PATRIOT Act** vom 26.10.2001 steht als Abkürzung für „***P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism*" Act of 2001

Die hiermit verbundenen *National Security Letters* begründen das Interesse an Zugriffen auf relevante Daten wie folgt: *„to protect against international terrorism or clandestine intelligence activities"*.
Durch den PATRIOT Act könne das *FB US-Metadaten ohne Gerichtsbeschluss anfordern.

2.) 2007 folgte der „**Protect America Act**" (**PAA**),

der das Abhören jeglicher Kommunikation erlaube, die ihren Ursprung oder ihr Ziel in den USA habe – ohne Gerichtsbeschluss.
Aus dem PAA 50USC 1805b sei folgender Auszug zitiert:
„the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communication service provider".

3.) Den **Foreign Intelligence Surveillance Act** (**FISA**) gibt es bereits seit 1978.

(Bekanntermaßen wurden auf Grundlage dieses Gesetzes und mit der Genehmigung von FISA-Gerichten über US-Server laufende Kommunikation abgehört.)

Hiernach wendete sich Prof. Roth näher eigenen Maßnahmen des Users zum Datenschutz wie insbesondere einer ausreichenden Verschlüsselung zu. Der Schutz persönlicher Daten gegen Auswertung durch Dritte sei nur durch Verschlüsselung an der Datenquelle möglich. Dies schütze die Information sowohl auf dem Datentransportweg als auch im gespeicherten Zustand.
Metadaten (also die zur Datenübermittlung notwendigen Verbindungsdaten) werden aber auch weiterhin ungeschützt übertragen. Es sei zwar eine weniger einsehbare Adressierung über Verwendung von nicht öffentlich (kenntlich gemachten) Servern technisch möglich. Speziell hierzu gab es ein deutsches Forschungsprojekt, das aber keine Forschungsförderungsgelder erhalten hatte.
Es wurden verschiedene Anbieter von Verschlüsselungssoftware und deren Leistungsfähigkeit miteinander verglichen: Hier stach der Anbieter (LaCie) mit der Software Wuala aus der Schweiz mit dem höchsten Verschlüsselungsgrad heraus.
Weiterhin erinnerte Prof. Roth daran, dass E-Mails meistens in einer Cloud liegen und eine E-Mail gemeinhin öffentlicher als eine Postkarte sei. E-Mails werden eventuell über in den USA stehende Server weitergeleitet oder verarbeitet, auch wenn ihr Ursprung außerhalb der USA liege. Hier greifen in aller Regel die angesprochen US-Gesetzgebungen PAA und FISA.
Bei Netzanbietern, die ihren Sitz in Deutschland haben [wie etwa der 1&1-Anbieter in Karlsruhe], können potenziell immer noch Programme wie Tempora und Prism greifen.

Eine wirksame Verschlüsselung müsse einen hinreichend starken Algorithmus haben (wie AES, 3DES [also ein dreifacher DES], oder Blowfish). Diese seien in absehbarer Zeit kaum zu entschlüsseln.
Weiterhin sollte der Schlüssel selbst erstellt sein sowie hinreichend lang sein (also mind. 128 bit), was bei den drei genannten Anbietern gegeben sei; RSA setzt sogar 2048 bit ein.
Der Schlüssel müsse aus einer zufälligen bit-Folge bestehen und natürlich sicher aufbewahrt werden.
Das verwendete Verschlüsselungsprogramm müsse zudem frei von Backdoors und Programmierfehlern sein.
Unter all diesen Voraussetzungen sei die Verschlüsselung sicher – nach dem Stand der Technik.

Die markanten Probleme bei der Verschlüsselung seien,

- den Schlüssel selbst zu erzeugen (oder wenigstens mit Zertifikat zu erwerben),
- eine Schlüsselverteilung mit Zertifikaten, die oft kostenpflichtig seien, während die Sicherheit allein abhängig von der Vertrauenswürdigkeit des Zertifikatanbieters sei
- sowie die Schlüsselüberprüfung durch Zertifikatssignatur.

Bei der Open PGP-Verschlüsselung werden die Schlüssel selbst erzeugt und selbst verschickt, auch ein Schlüsselserver für die Verschlüsselung sei verfügbar.
Open PGP sei verfügbar für folgende E-Mail-Programme: thunderbird, Evolution, KMail sowie als GpG4Win auch für Outlook.

Für das Signieren von E-Mails können Smime und OpenPGP verwendet werden, die auf Wunsch Signaturen (also digitale Unterschriften) für E-Mails erzeugen.
Hiernach lieferte Prof. Roth eine Kurzanleitung zur Installation von thunderbird sowie Tipps zum Herunterladen der LaCie Wuala-Cloud, die eine automatische Verschlüsselung biete und bei der fünf Gigabite Speicher kostenlos verfügbar seien.

An den in der BRD und auf internationaler Ebene verbrieften Grundrechtsschutz für selbstbestimmte Kommunikation der Bürgerinnen und Bürger erinnert Prof. Dr. Martin Kutscha, der bis zu seinem Ruhestand an der Hochschule für Wirtschaft und Recht in Berlin lehrte.
Zunächst stellt Prof. Kutscha die einschlägigen Regelungen auf Bundesebene zusammen. Insbesondere zur in der Verwaltung eingesetzten Informationstechnik hält er fest, dass die Exekutive bzw. die „vollziehende Gewalt" laut Art. 20 Abs. 3 GG selbstverständlich an Gesetz und Recht gebunden sind.

Zur Beantwortung der juristischen Frage nach Rechtsverletzungen durch Auswertungen unserer Daten (ohne eigene explizite Zustimmung) weist Prof. Kutscha zuerst auf das Recht auf **Informationelle Selbstbestimmung** hin, das 1983 durch das Urteil des Bundesverfassungsgerichts zur Volkszählung explizit ausformuliert wurde. Es sei Bestandteil des allgemeinen Persönlichkeitsrechts, das aus Art 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG abgeleitet wird.
Das **Fernmeldegeheimnis** bzw. das Telekommunikationsgeheimnis (Art. 10 GG) als aktueller Rechtsbegriff gilt abhängig davon, wo eine E-Mail gerade gespeichert sei: Wenn der Übertragungsvorgang abgeschlossen und die Nachricht auf dem eigenen PC oder Handy gespeichert sei, greife nicht mehr Art. 10 GG ein, sondern das Informationelle Selbstbestimmungsrecht. Wenn die E-Mail hingegen im Internet gespeichert sei, ändere sich die rechtliche Situation.
Aus diesen wenig realitätsnahen Unterscheidungen werde ersichtlich, dass ein *modernes grundrechtliches Schutzsystem klarer formuliert sein müsse*.
Vom Bundesverfassungsgericht kürzlich entwickelt wurde das Recht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme".
Für Daten, die ohne das Wissen des Nutzers erhoben worden sind (wie beispielsweise über Cookies, IP-Adressen etc.) greift eigentlich das Recht auf Informationelle Selbstbestimmung, zudem der bereits hinreichende **Art. 10 GG** als Abwehrrechte gegenüber der deutschen Staatsgewalt. Bei durch ausländische Akteure wie Nachrichtendienste oder private Unternehmen (wie beispielsweise Internet-Dienstleister) ohne Zustimmung des Betroffenen gewonnenen Daten begründen diese Rechte auch eine Schutzpflicht des Staates zugunsten der IT-Nutzer gegenüber solchen Dritten.

Auf EU-Ebene hat der Europäische Gerichtshof am 8. April 2014 das Urteil gegen die Vorratsdatenspeicherung getroffen. Als „Messlatte" diente ihm dabei die EU-Grundrechtecharta (aus dem Jahr 2000), genauer Art. 7 zur Achtung des Privatlebens und der Kommunikation sowie Art. 8 als Grundrecht auf Datenschutz („Schutz personenbezogener Daten") Das Gericht habe hiermit quasi das Bundesverfassungsgerichtsurteil zur Vorratsdatenspeicherung von 2010 fortgeschrieben.
Hier sei zu bedenken, dass **Metadaten**, also Verbindungs- bzw. Verkehrsdaten (also die Verknüpfung der Daten der Gesprächspartner, Verbindungszeit und –ort) ebenso aussagekräftig seien , da soziale Beziehungen transparent gemacht werden können.
Wie bereits im vorangegangenen Vortrag gehört, ist es technisch äußerst aufwendig, Metadaten zu verschlüsseln. Diese Daten werden von den Geheimdiensten wie auch von der Polizei im Rahmen von Strafverfahren genutzt.

Seit 1950 gilt auf europäischer Ebene die **Europäische Menschenrechtskonvention (EMRK)**, die inzwischen 47, also praktisch alle europäischen Staaten ratifiziert haben. Art. 8 der EMRK befasst sich mit dem Schutz der Privatsphäre der Bürger.
Angesichts fehlender Kontrolle und hoher Missbrauchsgefahren werden für neue Technologien, die für technische Überwachung geeignet sind, dringend neue detaillierte Regelungen notwendig. Die Regelungen müssen ausreichend bestimmt sein und der Bevölkerung angemessene Hinweise geben, wann auf ihre Daten zurückgegriffen werde.
Auf Grundlage der EMRK agiert der Europäische Gerichtshof für Menschenrechte in Straßburg, er wurde vom Europarat installiert, also nicht durch EU-Institutionen, und soll die Einhaltung der EMRK einklagbar machen.

Auch den US-Sicherheitsgesetzen wie dem PATRIOT Act und den innerhalb der USA divergierenden Gerichtsurteilen zu Datenschutzrechten steht der international übergreifende „**Pakt über bürgerliche und politische Rechte**“ von 1966 gegenüber. In diesem **UNO-Zivilpakt** befasst sich Art. 17 mit dem „Schutz der Privatsphäre und der Korrespondenz“.
Es gibt kein Gericht, das die Einhaltung dieser Rechte überwacht, dafür aber den Menschenrechtsrat sowie den Menschenrechtsausschuss der UNO.
Zur regelmäßigen Kontrolle der Menschenrechtslage in den Staaten, die den Pakt ratifiziert haben, geben diese in Abständen von mehreren Jahre Berichte hierüber an die UNO-Organe. Der letzte Jahresbericht der USA ist vor dem Hintergrund der Snowden-Veröffentlichungen scharf kritisiert worden.
Bei Verstößen gegen diesen UNO-Zivilpakt kann also höchstens eine öffentliche Pranger-Wirkung hergestellt werden, es gibt aber keine automatischen Sanktionsmöglichkeiten, die etwa über Gerichtsbeschlüsse durchgesetzt werden könnten.
Zu dem oben angesprochenen Art. 17 zum Schutz der Privatsphäre und der Korrespondenz gibt es einen „General Comment“ der damaligen Menschenrechtskommission der UN von 1988, die inhaltlich besagt, dass die Überwachung der Telekommunikation mit elektronischen Mitteln etc. verboten werden sollte.

Eine Standardforderung des Datenschutzes sei zudem, dass jeder Mensch das Recht haben sollte, zu erfahren, welche Daten zu welchem Zweck in welcher Datenbank gespeichert werden.
Zu den Allgemeinen Geschäftsbedingungen (AGB) von facebook lässt sich kritisieren, dass Verträge transparent gestaltet sein sollten; diese Grundanforderung ist in der BRD durch §305 BGB gesetzlich festgeschrieben. Das BGB sei natürlich ein territorial begrenztes Recht, reiche somit zur Regulierung von internationalen Datenströmen nicht aus.
Es sollte eine die modernen technischen Möglichkeiten berücksichtigende internationale Rechtsgrundlage für ein internationales Datenschutzrecht verabschiedet werden.
Die EU-Datenschutzgrundverordnung konnte bisher nicht verabschiedet werden aufgrund von Widerständen von Lobbygruppen.
Als Hintergrundinteresse kann davon ausgegangen werden, dass das jeweilige Geschäftsmodell einiger Unternehmen und Lobbyisten auf einem Datenverkauf auf Grundlage extrem schwacher Datenschutzgesetze basiere. (So habe sich facebook vor diesem Hintergrund als Sitz seiner Tochtergesellschaft in der EU mit Bedacht Irland ausgewählt.) Hinzu kommen die Interessen der *GeDe in die gleichlautende Richtung.
Diesen Interessen steht die Freiheit in einer Demokratie gegenüber, unbeobachtet handeln zu können – als Grundlage der Demokratie.

Heutige technische Entwicklungen ermöglichten bereits den vollen Zugriff auf alle Datenarten der Kommunikation.
Das Gewicht der Grund- und Menschenrechte muss durch der technologischen Entwicklung angepasste Gesetze weiterhin voll zum Tragen kommen.
Der Druck müsse „von unten“ kommen – von Netz-Bürgern und den Millionen Usern.
Erst durch politischen Druck ändere sich etwas.

Zuhörerfragen richteten sich zunächst noch einmal auf die genaueren Interessen an den Nutzerdaten. Die Interessen an den Nutzerdaten hätten unterschiedliche Hintergründe. Zunächst gäbe es das ökonomische Interesse an den Daten (etwa als Ware), die ein im Internet agierendes Unternehmen als Gegenleistung für seine Dienstleistung anfragen könne. Zudem gäbe es das historisch bestehende Interesse der Geheimdienste gegenüber den Bürgern.
Um die kritischen Folgen eines übersteigerten Interesses an der Privatsphäre zu verdeutlichen, wurde das theoretische Modell des Panoptikums von Bentham angeführt, einer Lebenssituation der ständigen (tatsächlichen oder vermuteten) Beobachtung. Die Beobachteten reagierten mit einer vorauseilenden Verhaltensanpassung.
Das Bestreben staatlicher Stellen, möglichst viel über Bürger wissen zu wollen sei erkennbar. Hier könnte es etwa auch das Informationsinteresse daran geben, was geschehen bzw. verändert werden müsse, um beispielsweise Wahlen zu gewinnen.
Eine weitere Frage zielte auf den UN-Menschenrechtsrat mit wechselndem Vorsitz ab, in dem auch autoritäre Staaten sitzen. Kutscha konterte, dass es um eine gemeinsame Rechtsgrundlage gehe, um gemeinsame Menschenrechtsstandards unabhängig von nationalen Traditionen. Das Ziel sei die Verbindlichkeit dieser Regelungen. Die Menschenrechte harren ihrer Durchsetzung. Auch das Recht, nicht überwacht zu werden, sollte geschützt werden.

Eine weitere Meldung verwies auf das Interesse an statistischen Daten für Planungsarbeiten, die aus der Eigenlogik von Planung und Verwaltung erwachse. Die Datenquellen werden zunehmend genauer und verknüpfter. Kutscha verwies hier im Kern auf eine veränderte Verfügbarkeit der Daten für Dritte. – Und führte als grundlegenden Meilenstein das Volkszählungsurteil des Bundesverfassungsgerichts von 1983 an. Hier sollte ein Abgleich des Melderegisters mit den Volkszählungsdaten abgewehrt werden aufgrund des Unbehagens der Bevölkerung. Damals musste sich der Staat die Daten beim Bürger holen, die Bürger konnten im Prinzip die Datenherausgabe praktisch verweigern. Heute ist hingegen bereits durch die Nutzung verbreiteter Technologien die Datenherausgabe praktisch gleich inklusive, während die Techniknutzung kaum vermieden werden könne.
Es gäbe zwar ein Grundbewusstsein auch der jungen Nutzer, das sich etwa darin zeige, dass 80% das höchste Level an Privatsphäre bei Internetdienstleistern wie facebook einstellten, die Daten werden aber trotzdem ausgewertet. Heute gäbe es weniger Widerstand der Bevölkerung bei der Datenerhebung. Die Möglichkeiten, die Daten zu nutzen, seien aber mittlerweile viel weitergehend gegeben.

Es gäbe aber verschiedene Ebenen, auf der Datenschutz und die Datensicherheit wieder gestärkt werden können. Etwa über die Unterstützung von Nichtregierungsorganisationen (NGO), die sich für diese Interessen einsetzten.

Technisch könnten sich etwa über die Regionalisierung des Internets bessere Schutzmöglichkeiten für Bürgerdaten erreichen lassen. So könnten E-Mails von deutschen Providern etwa nur in Europa herumgeschickt werden. Tatsächlich sei der technische Standard heute quasi nur von US-Firmen dominiert. Datenschutzinteressen setzen heute auch an solchen technischen Grundvoraussetzungen an.

5.) Rechtsanwalt Andreas Göbel, Fachhochschule Südwestfalen: „Wie kann Datenschutz effektiver aussehen? Eine rechtliche Bewertung“

Rechtsanwalt Andreas Göbel von der Fachhochschule Südwestfalen befasst sich mit der Frage, wie Datenschutz aus der juristischen Perspektive effektiver gestaltet und auch praktisch umgesetzt werden könne.

1.) Gesetzliche Bestimmungen, Sanktionen und faktische Lücken

Er verweist auf die bestehenden Gesetzgebungen insbesondere in Form der **Datenschutzgesetze**, die auch **Sanktionen** wie Bußgeldtatbestände bis zu 300000 € oder auch Freiheitsstrafen bis zu 2 Jahren beinhalteten.
Dennoch **bestehende Lücken praktischer und rechtlicher Natur** nennt Göbel anschließend exemplarisch. Ausnahmen des Datenschutzes wurden u.a. durch das Bundesdatenschutzgesetz selbst, etwa zu Forschungszwecken ermöglicht. Grundsätzlich müsse jede Änderung eines vorgegebenen Zweckes einer Datennutzung dokumentiert werden, beispielsweise, wenn Rechnungsdaten zu Werbezwecken verwendet werden.
Datenbestände fallen aufgrund technischer Grundlagen oft sowieso an, ohne dass sie extra gesammelt werden müssten. Meist sind die Datenbestände kaum verschlüsselt. Letztendlich liege es im Interesse vieler Unternehmen; sich Daten zu beschaffen und zu nutzen.

2.) Das Territorialitätsprinzip

Bei der **kommenden EU-Regulierung** zum Datenschutz handele es sich um eine **Grundverordnung**, die somit 1:1 von den Mitgliedsstaaten umgesetzt werden müsse, ohne dass hierbei ein eigenständiger Gestaltungsspielraum vorgesehen wäre.
Hier sollte das **Territorialitätsprinzip** eine wesentliche Rolle spielen: Es mache einen entscheidenden Unterschied, ob beispielsweise ein US-Konzern in der EU verklagt werden könne - insbesondere vor dem Hintergrund, dass wir etwa mit Irland ein **Zwangsvollstreckungsabkommen** abgeschlossen haben, nicht aber mit den USA.
In Deutschland und der EU werde bislang noch versucht, den Datenschutz etwas zu schützen im Vergleich zu vielen anderen Ländern. So wäre es ein maßgebliches Ziel, dass **Server nicht ausweichen in in dieser Hinsicht vergleichsweise relativ rechtsfreiere Räume**. Auch das Save-Harbour-Abkommen mit den USA habe seine Schwachpunkte.
Am besten für den Datenschutz sei es, „zu Hause zu bleiben“ und die **Datenschutzregelungen des eigenen Rechtsbereichs greifen zu lassen**. Auf diese Weise greife im Wesentlichen das **Territorialitätsprinzip** und biete einen relativ verlässlichen und steuerbaren Schutz.

Mit einer im Unternehmenssektor wichtigen deutschen Datenschutzregelung und deren praktischer Umsetzung beschäftigt sich Rechtsanwalt Göbel im Folgenden: den **betrieblichen Datenschutzbeauftragten**.
Eine nicht selten gemachte Beobachtung sei es, dass Unternehmen zunächst die Kosten für einen betrieblichen Datenschutzbeauftragten scheuten, spätestens aber dann reagierten, wenn sie vom Landesdatenschutzbeauftragten angeschrieben werden.

Bis vor fünf Jahren war die Ernennung eines betrieblichen Datenschutzbeauftragten eher eine definitorische Formsache, dem Mitarbeiter mit dieser Zusatzfunktion wurden kaum einschlägige Aktionen abverlangt. Demgegenüber erfolge die Ernennung heute oftmals unter deutlicher spürbarem Druck durch den (jeweiligen) Landesdatenschutzbeauftragten. Die **rechtliche Pflicht zur Ernennung von betrieblichen Datenschutzbeauftragten** erfolge nur aufgrund der Unternehmensgröße (oberhalb von 15 Mitarbeitern), **nicht aber aufgrund des Grades der jeweiligen Sensibilität der Daten**, die im betrieblichen Ablauf verarbeitet bzw. erhoben werden wie insbesondere auch bei Rechtsanwälten, Ärzten, etc..

3.) Arbeitnehmerdatenschutzgesetz: klar formulierte und strukturierte gesetzliche Regelungen

Das **Arbeitnehmerdatenschutzgesetz** bot in Deutschland bis Anfang 2013 **klare und sinnvolle Regelungen**, bis es im **Januar 2013 von Regierungsseite zurückgenommen** wurde. Es habe bisherige Urteile insbesondere des Bundesarbeitsgerichts übersichtlich abgebildet und einen Katalog von einschlägigen Situationen zum Nachschlagen geliefert, der für den Anwender in übersichtlicher Weise und rechtssicher anzuwenden war. **Mit** der **Aufhebung** des Arbeitnehmerdatenschutzgesetzes wurde der Anwender in eine sehr **unübersichtliche Situation** befördert, in der er wieder nur auf die erfolgten Gerichtsurteile, auf die Regelungen zur Nutzung personenbezogener Daten aus dem Bundesdatenschutzgesetz zurückgreifen könne. Nun kommen den Rechtsanwälten die Aufgaben zu, Einwilligungserklärungen für Nutzer zu verfassen nach verschiedenen Nutzungsparametern, anstatt auf das vorherige übersichtliche Arbeitnehmerdatenschutzgesetz zugreifen zu können.

4.) Mehr Kontrolle

Der nächste Ansatzpunkt von Göbel setzt auf mehr Kontrolle durch Landesdatenschutzbeauftragten, ohne dabei zu viel Aufwand zu verlangen. So schreibe der Landesdatenschutzbeauftragte von Nordrheinwestfalen beispielsweise stichprobenartig per Fragebogen Berufsgruppen wie Headhunter an, um hier etwas Kontrolle umzusetzen.
Nach Meinung von Rechtsanwalt Göbel müssten auch einzelne „Hindernisse abgebaut“ werden, die Arbeitgebern mitunter als zu übertrieben erschienen. So werde tatsächlich in Frage gestellt oder als Unsinn abgetan, eine schriftliche Einwilligung des Arbeitnehmers zur Verwendung dessen Daten einholen zu müssen.
Eine Regelung zur Löschung von Daten solle in einer EU-Datenschutzverordnung verankert werden.

Auf die Frage nach einer effektiveren Gestaltung des Datenschutzes im Hinblick auf private Unternehmen verweist Göbel darauf, das 300 Tausend € Bußgeld je einmaligem Verstoß selbst für google eine Strafe darstelle.
Zudem seien der PATRIOT Act und das (deutsche) Datenschutzrecht nicht miteinander vereinbar. Eine **technische Lösung** des Problems sei, ein **eigenes Rechenzentrum in Europa** aufzubauen, das nicht von Microsoft betrieben werde. Dies eröffne auch neue Geschäftsmodelle in der EU. Ein Rechenzentrum in der EU biete dann mehr Datenschutz, wenn Niederlassungen in den USA keinen Zugriff auf das in der EU sitzende Rechenzentrum haben.