Hausarbeit

.

am Institut für Mathematik und Informatik
der Universität Leipzig
über das Thema

Entwicklung des Datenschutzes in Deutschland seit 1949

.

vorgelegt von

Sebastian May

Mat.Nr.: 2591869

Referent: Dr. Hans-Gert Gräbe, apl. Prof.

Korreferent: Ken-Pierre Kleemann

Leipzig
30.09.2015

Inhaltsverzeichnis

Einleitung

Spätestens nach dem Skandal um den Bundesnachrichtendienst (BND) und die National Security Agency (NSA) ist das Thema Datenschutz wieder aktuell. Im April wurde bekannt, dass der BND über Jahre hinweg im In- und Ausland Bürger und Unternehmen ausspionierte und die gewonnenen Informationen an die NSA weiterleitete. Für viele Menschen bedeutete dies einen Eingriff in ihr Recht auf den Schutz ihrer persönlichen Daten, auch wenn das sogenannte G-10-Gesetz die Aufzeichnung durch den BND und die Weitergabe an ausländische Geheimdienste wie die NSA erlaubt. Viele Bürger sind besorg, ob ihre gespeicherten Daten noch sicher sind, an wen sie übermittelt und zu welchen Zwecken sie verwendet werden.

In der Folgenden Arbeit soll untersucht werden, wie sich der Datenschutz Rechtlich und in seiner Umsetzung in Deutschland entwickelt hat. Als Beginn der Untersuchungen wurde 1949 gewählt, da sich zu der Zeit im geteilten Deutschland zwei klare Vorgehen im Umgang mit Datenschutz hervorhoben. Des Weiteren soll erforscht werden, inwieweit sich der digitale Wandel auf den Datenschutz auswirkt. Schlussendlich soll überlegt werden, warum Daten gesammelt werden und welche Gefahren, aber auch welches Potential dadurch entsteht.

1. Begriffsklärung

Zu Beginn sollte geklärt werden, wie der Begriff ‚Datenschutz' im Weiteren verwendet wird. Im Duden findet sich so Beispielsweise die Definition ‚Schutz des Bürgers vor Beeinträchtigung seiner Privatsphäre durch unbefugte Erhebung, Speicherung und Weitergabe von Daten, die seine Person betreffen'. Um diese Definition etwas zu präzisieren soll der Ursprung des Wortes ‚Datenschutz' etwas näher betrachtet werden.

1890 wurde in den USA die erste Publikation zum Thema privacy (dt. = Privatsphäre) von Samuel Warren und Louis Brandeis verfasst und veröffentlicht (‚The Right to Privacy'), welche maßgeblichen Einfluss auf die Rechtsentwicklung in den USA hatte, vor allem was das Menschenrecht angeht. Hierin wurden erste nähere Erklärungen über die Bedeutung des Wortes ‚Privatsphäre' getätigt. Übersetzen lässt sich diese Erklärung folgendermaßen: ‚Jedem Individuum steht das Recht zu zu bestimmen, inwieweit seine Gedanken, Meinungen, Gefühle und Personenbezogene Informationen anderen mitgeteilt werden sollen. ' (Vergleich https://en.wikipedia.org/wiki/The_Right_to_Privacy_(article)).

In den 1960er Jahren plante der damalige US-Präsident John F. Kennedy die Einrichtung eines nationalen Datenzentrums, um dort eine Registrierung jedes US-Bürgers durchzuführen. Der Vorschlag sorgte international für Aufsehen und wurde auch in Deutschland diskutiert. Um das in der Debatte häufig gebrauchte Wort ‚privacy' – mit der Bedeutung nach Warren/Brandeis – ins deutsche zu übersetzen, wurde das Wort ‚Datenschutz' eigeführt, welches heute auch in anderen Sprachen gebräuchlich ist (z.B. data protection oder protection des données) (Vergleich https://de.wikipedia.org/wiki/Datenschutz#Geschichte).

Die Verwendung des Wortes Datenschutz im Folgenden bezieht sich demnach auf seine Herkunft und damit auf die Ursprünglich von Warren/Brandeis eingeführte Definition. Damit bezeichnet Datenschutz vor allem das Recht auf eine Selbstbestimmung über Gedanken, Meinungen und – hier hauptsächlich verwendet – personenbezogene Daten.

2. Geschichtliche Entwicklung

Um Herauszufinden inwieweit sich der Datenschutz in Deutschland durch den digitalen Wandel verändert hat, muss zunächst die historische Ausgangslage und damit die Zeit vor diesem Wandel betrachtet werden.

1949 entstanden in Deutschland aus den 4 Besatzungszonen die BRD und die DDR. Deshalb ist eine Betrachtung der Entwicklung an dieser Stelle differenziert durchzuführen.

2.1 DDR

In der DDR wurde 1950 das Ministerium für Staatssicherheit gegründet, welches vor allem eine Stellung als Geheimdienst und Ermittlungsbehörde einnahm, jedoch vor allem durch die Überwachung der Bürger bekannt ist. Unter dem Vorwand die DDR vor Spionen, Saboteuren und ‚Terroristen' zu schützen wurden Daten über die Bürger in großen Mengen gesammelt. Rechtlich war der Datenschutz sowohl in den Bestimmungen der Vereinten Nationen (‚Niemand darf willkürlichen Eingriffen in sein Privatleben […] und seinen Schriftverkehr […] ausgesetzt werden' – Artikel 12), als auch in der Verfassung der DDR verankert (‚Post- und Fernmeldegeheimnis sind unverletzbar' – Artikel 31). Das MfS war allerdings ein staatliches Organ, welches direkt unter der Regierung stand und deshalb in seinen Rechten nur wenige Einschränkungen hatte. (Vergleich https://de.wikipedia.org/wiki/Ministerium_f%C3%BCr_Staatssicherheit)

Die Vielfalt der Methoden zur Überwachung und Datenbeschaffung wurde schon damals durch den Fortschritt in Wissenschaft und Technik hervorgerufen. So untersuchte die amerikanische Autorin Kristie Macrakis die vom CIA aufgedeckten Methoden, die von vom MfS zur hierfür verwendet wurden. Dazu zählen unter anderem eine Vielzahl von kompakten Mikrofonen, vor allem für die Verwendung in Wanzen oder eigens entwickelte Objektive für Kameras zur Fotographie aus großer Entfernung oder um Ecken. Da ein großer Anteil an zwischenmenschlicher Kommunikation über Brief-, Telegramm- und

Telefonverkehr stattfand, lag hier ein besonderes Interesse zur Beschaffung von Daten. So gab es z.B. Telefonabhöranlagen mit der Möglichkeit der Speicherung auf damals handelsübliche Kassetten sowie einem Zeitstempel für die genaue Dokumentation. Marakis fand außerdem für die Überwachung des Briefverkehrs eine Vielzahl technischer Geräte. Heißluftgebläse und automatische Schließmaschinen für das unbemerkte öffnen von Briefen sowie Fototische zur Ablichtung von Briefen z.B. für die Erfassung von Handschriften. Des Weiteren wurde eigens ein Gerät zum parallelen Aufzeichnen von Telegrammen Entwickelt. (Vgl. Macrakis ‚Die Stasi-Geheimnisse: Methoden und Technik der DDR-Spionage'). In den 1970er Jahren wurde auch die Methode der Geruchsdifferenzierung durch das MfS durchgeführt. Geruchsdifferenzierung bezeichnet hierbei ein Vorgehen, bei dem Geruchsproben (z.B. von Briefen, persönlichen Gegenständen, etc.) durch Sterile Tücher aufgenommen und dann luftdicht verschlossen wurden. Diese Gerüche konnten später von speziell ausgebildeten ‚Differenzierungshunden' aufgenommen werden, um die zugehörige Person zu identifizieren. Auch die zunehmende Entwicklung der Computertechnik hatte Einfluss auf die Überwachungsmöglichkeiten. So wurde der 1988 auf den Markt gebrachte BSP-12 Computer, welcher in der Lage war Einzelbilder aus Videos zu schneiden und auf Kassette zu speichern, hauptsächlich vom MfS gekauft (Vergleich https://de.wikipedia.org/wiki/BSP-12).

Es zeigt sich hier, dass das Thema Datenschutz zwar rechtlich gesehen in den Verfassungen der UN und der DDR vertreten war, die Realität jedoch stark von deren Umsetzung und Einhaltung entfernt war. Die angewendeten Methoden wurden auch damals schon durch den technologischen Fortschritt und die beginnende Automatisierung durch Computer ermöglicht und verbessert.

2.2 BRD

In der ehemaligen BRD wurde das Thema Datenschutz im rechtlichen Sinne sehr ausgiebig behandelt. So wurde 1970 das Hessische Datenschutzgesetz veröffentlicht, das erste formelle Datenschutzgesetz der Welt. Verfasst von Spiros Simitis, einem griechischen Rechtswissenschaftler, regelte dieses Gesetz

die Verwaltung und Verwendung von personenbezogenen Daten. So sollte sichergestellt werden, dass das Recht auf informationelle Selbstbestimmung nicht verletzt wird. Damals fehlten allerdings noch Regelungen, welche für unser heutiges Verständnis von Datenschutz unverzichtbar sind. So gab es beispielsweise noch kein Verbot für die Aufnahme von Daten ohne Einwilligung der betroffenen Person. Personenbezogene Daten durften auch dann aufgenommen und gesichert werden, wenn sie für die Arbeit der Behörde nicht zwingend relevant waren (Vergleich https://de.wikipedia.org/wiki/Hessisches_Datenschutzgesetz).

1797 wurde in Hessen der erste Landesdatenschutzbeauftragte – Willi Birkelbach – eingestellt. Seine Aufgaben bestanden darin zu kontrollieren, ob die bestehenden Datenschutzbestimmungen eingehalten werden. Außerdem sollte erforscht werden, wie sich die zunehmende Automatisierung von Vorgängen auf den Datenschutz auswirkt. 1975 wurde diese Stelle von Simitis übernommen, welcher 1977 auch für die neu geschaffene Stelle als Bundesdatenschutzbeauftragten in Betracht gezogen wurde (Vergleich https://de.wikipedia.org/wiki/Hessischer_Datenschutzbeauftragter).

Der Bundesdatenschutzbeauftragte sollte Bundesbehörden und öffentliche Stellen (vor allem Telekommunikations- und Postdienstunternehmen) beraten und dahin kontrollieren, dass die bestehenden Datenschutzgesetze eingehalten werden. An dieser Stelle zeigt sich, dass das Thema Datenschutz ähnlich wie in der DDR gesetzlich festgehalten wurde, in der BRD allerdings Stellen und Institutionen zur Kontrolle der Einhaltung selbiger bestanden (Vergleich https://de.wikipedia.org/wiki/Bundesbeauftragter_f%C3%BCr_den_Datenschutz_und_die_Informationsfreiheit).

1977 wurde auch das erste deutschlandweit geltende Datenschutzgesetz verabschiedet (Bundesdatenschutzgesetz oder BDSG). Dieses Orientierte sich stark an den bereits bestehenden Gesetzen die inhaltlich mit dem Thema verbunden waren (z.B. ärztliche Schweigepflicht, Beichtgeheimnis und Postgeheimnis) sowie an den Überlegungen zum Datenschutz im in Kapitel 1 erwähnten ‚The Right to Privacy' und dem Hessischen Datenschutzgesetz (vergleich https://de.wikipedia.org/wiki/Bundesdatenschutzgesetz).

1987 wurden wesentliche Mängel im Datenschutzgesetz sichtbar. Bereits 1981 sollte in Deutschland eine Volkszählung stattfinden um z.B. Pläne für soziale Versorgung, Verkehrswesen und Ähnliches zu verbessern. Nach einigen Verzögerungen kam es 1983 nach einer Vielzahl von Bürgerprotesten zu einem Verfahren vor dem Bundesverfassungsgericht gegen die Volkszählung. Die Klage richtete sich vor allem dagegen, dass die gesammelten Daten auf den Volkszählungsbögen Rückschlüsse auf die Identität der befragten Personen erlaubten. Am 15. Dezember 1983 kam es zum sogenannten ‚Volkszählungsurteil', bei dem das Bundesverfassungsgericht die geplante Volkszählung aufgrund des Verstoßes gegen das Grundrecht auf informationelle Selbstbestimmung als Verfassungswidrig erklärte. Die Befragungsbögen wurden bis 1987 so abgeändert, dass eine Identifikation der Befragten nicht mehr möglich war. Auch wurden in dem Zusammenhang die Datenschutzgesetze der Länder und des Bunden so geändert, dass die 1970 noch fehlenden Artikel zur Zweckmäßigkeit der Sammlung personenbezogener Daten ergänzt wurden. Spiros Simitis bezeichnete das Gesetz „weit über die Grenzen der Bundesrepublik Deutschland hinaus als der wohl wichtigste Beitrag zur Fortentwicklung des Datenschutzes."
(Vergleich https://de.wikipedia.org/wiki/Volksz%C3%A4hlungsurteil).

Neben den erheblichen Fortschritten – vor allem der rechtlichen Verankerung des Datenschutzes – gab es allerdings auch negative Entwicklungen, deren Auswirkungen heute deutlich spürbar sind.

Nach dem zweiten Weltkrieg verzichtete die BRD vorübergehend auf Notstandsgesetze. Diese Gesetze sollten ursprünglich dazu dienen in Krisenzeiten die Ordnung im Land aufrecht zu erhalten. Nachdem Artikel 48 der Weimarer Verfassung durch die Nationalsozialisten missbraucht wurde, wurden diese vorerst nicht im Besatzungsstatut der Alliierten aufgenommen. Erst 1968 wurde - damals unter großen Protesten der Opposition – die Deutschen Notstandsgesetze wieder in das Grundgesetz aufgenommen. In diesem Zusammenhang wurde unter anderem auch das sogenannte G-10-Gesetz verabschiedet. Dieses berechtigte den Bundesnachrichtendienst, Verfassungsschutzbehörden und den Militärischen Abschirmdienst dazu,

Telekommunikation und den Postweg zu überwachen. Dabei sind die entsprechenden Stellen dazu verpflichtet, diese Überwachung zu ermöglichen. Das G-10-Gesetz existiert heute noch und hatte maßgebliche Auswirkungen auf den Skandal um die NSA und den BND. Der Historiker Josef Foschepoth sagte 2014 dazu: „Der damalige Chef des Bundesamtes für Verfassungsschutz, Hubert Schrübbers sagte während der Abhöraffäre 1963, deutsche und amerikanische Geheimdienste seien ein einheitlicher Organismus.“ (Vergleich https://de.wikipedia.org/wiki/Artikel-10-Gesetz).

Betrachtet man das geteilte Deutschland nach dem 2. Weltkrieg als ganzes, so zeigen sich im Wesentlichen 2 Entwicklungen im Datenschutz. Zum einen wurde, vor allem in der DDR, systematische Kontrollen der Bevölkerung durchgeführt. Der damals schon wachsende Gebrauch und die Weiterentwicklung technischer Geräte hat die Abhörung in großem Stil begünstigt und in einigen Bereichen (wie z.B. der Telekommunikation) erst ermöglicht. Zum anderen wurden nach dem Beispiel der USA und der dort veröffentlichten Publikation ‚The Right to Privacy‘ die ersten Gesetze zum Datenschutz in die Verfassungen der Länder und des Bundes verabschiedet.

Da die Technologisierung nach dem 2. Weltkrieg zwar schon in Ansätzen vorhanden stattfand (z.B. in der Telekommunikation und der beginnenden Computertechnik), allerdings noch nicht im erheblichen Teilen Einfluss auf die Datenverarbeitung von Privatpersonen hatte, soll im Folgenden die Entwicklung des Datenschutzes vor allem im Rahmen des digitalen Wandels betrachtet werden.

3. Digitaler Wandel

Für die Untersuchung des Zusammenhangs zwischen digitalem Wandel und der Entwicklung des Datenschutzes in Deutschland muss vorher geklärt werden, was unter digitalem Wandel verstanden wird und wie sich dieser bemerkbar macht. Dazu sollen im Folgenden verschiedene Aspekte des Digitalen Wandels bzw. der

Digitalen Revolution betrachtet sowie deren Auswirkung auf den Datenschutz näher erläutert werden.

Als ‚Digitale Revolution' wird der Umbruch zum Ende des 20. Jahrhunderts bezeichnet, bei dem sich durch Digitalisierung und Automatisierung ein Großteil der Technik und viele Lebensbereiche stark geändert haben (Vergleich https://de.wikipedia.org/wiki/Digitale_Revolution).

3.1 Digitalisierung

Nach einem Artikel von Martin Hilbert und Priscila Lopez (http://www.sciencemag.org/content/332/6025/60) war es 2002 das erste Mal möglich, mehr Daten in digitaler als in analoger Form zu speichern. Laut Ihrer Schätzungen waren 2007 bereits 94% der weltweiten Informationen in digitaler Form abgespeichert. Auch die Telekommunikation fand bereits 2000 zu 98% digital statt. Auch lässt sich erkennen, dass die weltweit übertragene Datenmenge vor allem im Internet in kurzen Zeitabständen schnell vergrößert. Laut Studie der IEEE von 2015 (in Anlehnung an eine Studie der HSSG von 2007) wird angenommen, dass sich das übertragene Datenvolumen im Netz seit 2007 ca. alle 18 Monate verdoppelt. Damit verzehnfacht sich das Datenvolumen im Zeitraum von 2010 bis 2015 und laut Prognose der IEEE wird 2020 ein ca. 100-mal größeres Datenvolumen als 2010 vorausgesagt. Auch wenn laut Studie ein großer Teil dieses Anstiegs durch neue Technologien wie Internetfernsehen oder der Download von Speicherintensiveren Computer- und Konsolenspielen über das Internet zustande kommt, so zeigt sich vor allem in den Studien der HSSG, dass die Menge an Informationen im Netz einen extremen Anstieg verzeichnet (Vergleich http://www.golem.de/news/ieee-datenvolumen-im-internet-verdoppelt-sich-alle-zwei-jahre-1208-93957.html).

Hieraus lässt sich erkennen, dass die Digitalisierung (im Sinne der Verarbeitung von Informationen als digitale Daten) in den letzten 15 – 20 Jahren enorm fortgeschritten ist.

Ermöglicht wurde diese Entwicklung vor allem durch Fortschritte im technischen Bereich. Vor allem durch integrierte Schaltkreise wurden die Möglichkeiten zur Datenverarbeitung in den letzten Jahrzehnten in einem enormen Tempo vorangetrieben. Vergleicht man so beispielsweise die Cray 1, einen der ersten Supercomputer aus dem Jahr 1976, mit modernen Geräten, so wird schnell deutlich wie stark sich die Dimensionen im Bereich der Rechenleistung und Speicherkapazität geändert haben. Hatte die Cray 1 damals einen Speicher von 2 MByte und eine Taktrate von 10 MHz, so haben heutige Mobiltelefone wie z.B. das Iphone 5s von Apple mit 2,6 GHz und 64 GByte Speicher etwa das 1000-Fache an Leistung bei einem Bruchteil der Größe und des Gewichts (5,5 Tonnen zu 112 Gramm). (Vergleich https://de.wikipedia.org/wiki/Integrierter_Schaltkreis).

Hier zeigt sich, dass durch den technologischen Fortschritt die Möglichkeiten von Technik vor allem im privaten Gebrauch stark zugenommen haben. Dies zeigt sich ebenfalls an den Verkaufszahlen von Computern für den Privatgebrauch. So wurden im Zeitraum von 1974 – 1996 weltweit etwa 55 Mio. Computer in diesem Bereich gekauft (Quelle https://de.wikipedia.org/wiki/Heimcomputer), wohingegen laut Statistischem Bundesamt 2014 in Deutschland etwa 1,7 PCs (Notebooks und Laptops einbezogen) pro Haushalt vorhanden waren (Quelle https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/AusstattungGebrauchsguetern/Tabellen/Infotechnik_D.html).

Das Zusammenspiel aus technologischem Fortschritt und Digitalisierung hat im privaten Gebrauch die Funktion, das Leben in verschiedenen Bereichen einfacher zu gestalten. Neben Vorteilen wie geringerem Platzbedarf (z.B. beim Vergleich von Büchern in einer Bibliothek und deren Speicherung in digitaler Form auf einem EBook-Reader), und dem einfacheren Erstellen von verschiedenen Datenformaten (z.B. aufnehmen und Bearbeiten von Video und Musik) gibt es auch Faktoren, die einerseits Vorteile für den täglichen Gebrauch mit sich bringen, allerdings auch eine gezieltere und einfachere Überwachung ermöglichen. So kann in digitalen Daten sehr schnell und einfach nach bestimmten Begriffen gesucht werden. Welche Probleme das mit sich bringen kann zeigt der Fall von Andrej Holm. Holm ist ein deutscher

Sozialwissenschaftler, welcher sich vor allem mit Themen wie Stadterneuerung und Wohnungspolitik beschäftigt. 2007 wurde Holm wegen Verdachts auf Mitgliedschaft in einer terroristischen Vereinigung verhaftet. Als Grund für die Verhaftung wurde genannt, dass in seinem Emailverkehr und in seinen Suchanfragen im Internet häufig die Begriffe „Gentrification“ und „Prekarisierung“ vorkamen. Diese Begriffe wurden ebenfalls gehäuft in Emails und Suchanfragen einer linksradikalen kriminellen Vereinigung gefunden, weshalb Holm ebenfalls im Verdacht stand zu dieser Gruppe zu gehören. Viele auch international tätige Wissenschaftler zweifelten stark an der Zugehörigkeit Holms zu dieser Gruppe, vor allem da seine verwendeten Suchbegriffe durch das Themenfeld seiner Forschung bedingt waren. Holm wurde aufgrund fehlender Beweise bereits einen Monat später wieder freigelassen (Quelle https://de.wikipedia.org/wiki/Andrej_Holm).

Ein weiterer Faktor der Digitalisierung ist die unkomplizierte Langzeitspeicherung von Daten. Grade in Verbindung mit dem wesentlich geringeren Bedarf an Speicherplatz ist es möglich, enorme Mengen an Daten zu speichern. Dies hat dahingehend Einfluss auf den Datenschutz, dass beispielsweis die Vorratsdatenspeicherung ermöglicht wird. Unter Vorratsdatenspeicherung versteht man die Speicherung personenbezogener Daten durch öffentliche Stellen ohne einen aktuellen Nutzen dieser (vor allem Telekommunikationsdaten).

Begründet wird der Bedarf an einer Vorratsdatenspeicherung von Befürwortern vor allem durch die Anwendung bei Kriminalitäts- und Terrorismusbekämpfung. Durch Informationen die aus den Telekommunikationsdaten gewonnen werden können Rückschlüsse auf das soziale Netzwerk (im Sinne der sozialen Kontakte und Verbindungen einer Person) gezogen werden. So seinen bei den Anschlägen von Madrid 2004 vor allem durch die gespeicherten Telekommunikationsdaten eine Aufklärung gelungen. Das Bundeskriminalamt argumentiert hingegen, dass sich die Aufklärungsquote durch eine derartige Speicherung bestenfalls um 0,006% erhöhe (siehe http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-fuer-eine-0-006-Prozentpunkte-hoehere-Aufklaerungsquote-151466.html). Als weiterer Punkt

der Vorratsdatenspeicherung gilt die IP-Vorratsdatenspeicherung. Hierbei wird gespeichert, wann eine IP-Adresse für einen Internetanschluss verwendet wird. In Deutschland wurde dieser Vorschlag von der SPD zeitweise eingebracht, allerdings ebenfalls aus Gründen des Datenschutzes wieder verworfen. So können vor allem durch die gehäufte Verwendung von mobilen Endgeräten und deren Zugang zum Internet grobe Bewegungsprofile von Personen erstellt werden.

Bereits 2010 wurde in Deutschland der Versuch unternommen, eine Vorratsdatenspeicherung für Daten von Telekommunikationsanbietern durchzusetzen. Damals wurde der Vorschlag für ein Gesetz diesbezüglich vom Bundesverfassungsgericht gekippt, da es weder ausreichende Maßnahmen zur Sicherung der gespeicherten Daten gebe und außerdem ein Verstoß gegen Artikel 10 des Grundgesetzes („Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich“ Vergleich http://www.gesetze-im-internet.de/gg/art_10.html) gesehen wurde. Im Juni wurde in der SPD erneut die Zustimmung zu einem Gesetzesentwurf von Bundesjustizminister Heiko Maas gegeben. Dieses Gesetz soll 2018 evaluiert werden und die Speicherung von Telekommunikations- und Internetdaten über einen längeren Zeitraum ermöglichen. Maas selbst war bis 2013 noch verstärkt gegen eine solche Speicherung eingetreten, verfasste auf Drängen Sigmar Gabriels hin jedoch den Gesetzesentwurf und befürwortet heute die Vorratsdatenspeicherung (Vergleich http://www.zeit.de/politik/deutschland/2015-06/vorratsdatenspeicherung-spd-sigmar-gabriel).

Es zeigt sich, dass der Fortschritt im technischen Bereich und die Digitalisierung von Daten dazu geführt haben, dass immer mehr Informationen in elektronischer Form vorhanden sind. Das ermöglicht eine Speicherung von vielen Daten über einen langen Zeitraum sowie deren schnelle und gezielte Auswertung. Auch wenn durch die Gesetzgebung ein Recht auf die Selbstbestimmung im Bezug auf persönliche Daten besteht, so zeigt sich dennoch, dass diese Gesetze in bestimmten Fällen umgangen werden können (Beispielsweise durch G-10 oder die Vorratsdatenspeicherung).

3.2 Internetnutzung

1991 wurde das Internet erstmals für die weltweite Nutzung zur Verfügung gestellt. Inzwischen hat es in unseren Kulturkreisen einen nicht mehr wegzudenkenden Stellenwert eingenommen. Laut Statistischem Bundesamt nutzen im 1. Quartal 2014 etwa 80% der Personen ab 10 Jahren das Internet, 82% von ihnen jeden bzw. fast jeden Tag und 63% über mobile Endgeräte wie Laptops, Smartphones oder Tablet-PCs. Deshalb ist es wichtig, das Internet als beeinflussenden Faktor für den Datenschutz näher zu betrachten. Hierfür sollen besonders 3 Teilgebiete des Internets untersucht werden. Online-Transaktionen und Online-Märkte wie Beispielsweise Amazon oder EBay, Social Networks wie Facebook oder Twitter und zuletzt der Umgang mit internetfähigen Endgeräten. (Quelle:
https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/ITNutzung/Aktuell_ITNutzung.html)

3.2.1 Onlinehandel

Der Begriff Onlinehandel umfasst verschiedene Vorgänge, um im Internet Waren, Dienstleistungen und Ähnliches zu erwerben. Dazu zählen die Suche und das tatsächliche Erstehen der Ware inklusive deren elektronische Bezahlung. Nach einer Statistik von Sabine von Thenen (Quelle https://www.destatis.de/DE/Publikationen/WirtschaftStatistik/Informationsgesellschaft/ECommercePrivateHaushalte_82014.pdf?__blob=publicationFile) haben im Jahr 2013 bereits ca. 83% der Internetnutzer bereits Einkäufe über selbiges getätigt. Laut der Internetseite statista.com (http://de.statista.com/themen/757/amazon/) erreichte Amazon im Oktober 2014 Besucherzahlen von 24,8 Millionen, auf EBay waren es im März 2015 knapp 89,5 Millionen geschaltete Anzeigen allein in Deutschland (http://de.statista.com/statistik/daten/studie/157490/umfrage/anzahl-der-

auktionen-auf-ebay-in-ausgewaehlten-laendern/). Diese Zahlen zeigen, dass der Onlinehandel in Deutschland eine wichtige Rolle spielt.

Der eigentliche Einfluss auf den Datenschutz liegt hierbei bei den hinter dem Handel steckenden Prozessen. So stellte der Deutsche Händlerbund beispielsweise in einer Studie von 2014 fest, dass 41% aller Online-Shops gegen bestehende Datenschutzbestimmungen verstoßen. Vor allem durch Webcontrolling-Tools wird das Nutzungsverhalten beobachtet und Benutzerprofile erstellt, welche für Werbezwecke verwendet werden (siehe http://www.haendlerbund.de/datenschutz). Webcontrolling-Tools wie zum Beispiel Google Analytics untersuchen so unter Anderem von wo die Nutzer stammen, welche Seiten und welche Unterseiten über welchen Zeitraum besucht werden. Unter dem Ziel Werbestrategien, Produktplatzierung und andere Abläufe des Handels zu verbessern werden so persönliche Daten gesammelt. In Deutschland ist die Verwendung solcher Tools deshalb aus rechtlicher Sicht sehr Umstritten (Vergleich https://de.wikipedia.org/wiki/Web_Analytics), vor allem da diese Tools oftmals IP-Adressen ohne vorherige Nachfrage speichern, welche laut Datenschutzgesetz zu den personenbezogenen Daten zählen.

3.2.2 Social Networks

Der Begriff ‚Web 2.0' wurde 2003 von Eric Knorr erstmals verwendet. Er bezeichnet den Wandel im Gebrauch des Internets – weg von der klassischen Anbieter-Nutzer-Beziehung und hin zu Plattformen, deren Inhalte durch die Nutzer zur Verfügung gestellt werden. Dieser Wandel wird vor allem in Social Networks wie beispielsweise Youtube, Facebook und Twitter sichtbar. Diese Seiten bieten dem Nutzer lediglich die Oberfläche und übernehmen die Verwaltung, die eigentlichen Inhalte werden jedoch von den Nutzern bereitgestellt (z.B. im Rahmen von Videos und Kommentaren auf Youtube oder den Nutzerprofilen und Gruppen auf Facebook). Die Nutzerzahlen auf Facebook in Deutschland bewegten sich 2014 im Bereich um 28 Millionen (Quelle http://de.statista.com/statistik/daten/studie/70189/umfrage/nutzer-von-facebook-in-deutschland-seit-2009/). Welche Konflikte mit dem Datenschutz entstehen

können zeigt der Fall von Maximilian Schrems, einem österreichischem Datenschutzexperten. 2011 machte Schrems von seinem Recht auf die Herausgabe gespeicherter persönlicher Daten gebrauch und forderte die über ihn auf Facebook vorhandenen Daten ein. Gesendet bekam er knapp 1200 PDF-Seiten, zum Teil auch sehr vertrauliche Informationen aus privaten Chats und eigentlich gelöschte Daten. Er erstattete 22-mal Anzeige gegen den Konzern, unter anderem auch wegen der damals noch vorhandenen Option zur automatischen Gesichtserkennung, die bei geposteten Fotos die Freundesliste durchsucht und Vorschläge zur Verlinkung anbietet. Momentan läuft ein weiterer Prozess gegen Facebook von Schrems, da dieser die Rechtmäßigkeit der Übermittlung der Facebook-Daten aus Irland (Sitz von Facebook in Europa) in die USA bezweifelt. Das Urteil hierzu wird am 6. Oktober erwartet (Quelle http://www.heise.de/newsticker/meldung/Datenschutz-bei-Facebook-USA-widersprechen-EuGH-Generalanwalt-wegen-Safe-Harbour-2831242.html).

Aus Datenschutzrechtlicher Sicht befinden sich Social Networks oft in einer Grauzone. So werden die Daten meist freiwillig an Facebook, Twitter und Ähnliche abgegeben. Diese haben dann in Ihren Nutzungsbedingungen festgelegt, dass ihre Daten auch weitergegeben werden dürfen.Auf Facebook werden diese Bedingungen beispielsweise automatisch beim erstmaligen Einloggen akzeptiert, was dem deutschen Datenschutzrecht allerdings widerspricht, wogegen allerdings nur wenige wie Schrems rechtlich vorgehen. Wenn die Daten also von den Nutzern freiwillig zur Verfügung gestellt werden, dann in die USA übermittelt und dort unter weniger strengen Datenschutzbestimmungen bearbeitet und durchsucht werden, dann ist die Einhaltung des Datenschutzes in den einzelnen Ländern weitestgehend gewährleistet, auch wenn ein solches Vorgehen insgesamt in Deutschland nicht möglich wäre. (Quelle: Aufzeichnungen zum Seminar ‚Social Media in Schule und Unterricht‘ an der Universität Leipzig – Nietsche, Aust).

3.2.3 Mobile Endgeräte

2014 nutzen laut Statistik etwa 54% der Deutschen mobiles Internet (Quelle http://de.statista.com/statistik/daten/studie/197383/umfrage/mobile-internetnutzung-ueber-handy-in-deutschland/). Zu den beliebtesten Funktionen zählen demnach Social Networks und Navigationsdienste. Viele Apps benötigen mittlerweile ebenfalls eine Internetverbindung und häufig auch die Ortungsdienste des mobilen Endgerätes. Allgemein können Apps verschiedene Berechtigungen fordern, je nach Betriebssystem bei erstmaliger Verwendung auf Nachfrage oder bereits bei der Installation. Diese Berechtigungen erlauben es der App, verschiedene Funktionen des Smartphones oder Tablets zu nutzen. Neben den bereits erwähnten Funktionen wie Internetzugang oder der Bestimmung des Standortes können einer App auch die Möglichkeiten zum Anwählen von Telefonnummern, Versenden von Kurznachrichten, Aufnehmen von Ton, Bild oder Video oder dem Lesen, Ändern und Löschen von Speicherinhalten eingeräumt werden. Das diese Zugriffe bei einigen Apps nichts mit den eigentlich gegebenen Funktionen zu tun haben zeigt sich am Beispiel der App ‚Brightest Taschenlampe' im Android-Store. Mit der Installation auf dem Smartphone werden der App zum Beispiel die genaue Standortabfrage, der Zugriff auf Fotos, Medien und Dateien sowie der Abruf der bestehenden Internet-Verbindung ermöglicht – Funktionen die eine Taschenlampen-App sicherlich nicht dringend benötigt. (Quelle https://play.google.com/store/apps/details?id=goldenshorestechnologies.brightestflashlight.free). Dennoch wurde diese App bereits 1,25 Millionen Mal im Google-Playstore heruntergeladen. Wie eine Untersuchung zeigte verkauften die Programmierer der App die gesammelten Daten wie beispielsweise die Standorte der Nutzer und die eindeutigen Gerätekennungen an Werbeunternehmen. Damit wurden die AGBs eindeutig verletzt, da diese einen Verkauf der Daten an Dritte verneinten. Auch sammle die App die Daten bereits vor der eigentlichen Annahme der AGBs und die bestehende Option zur Deaktivierung der Datensammlung habe keinerlei Auswirkungen (Quelle http://www.giga.de/apps/google-play-store/news/taschenlampen-app-verkauft-ungefragt-daten-von-millionen-nutzern/). Hier wird ersichtlich, dass es vor allem in neueren technischen Anwendungsbereichen noch großen Bedarf zur Verbesserung des Datenschutzes bzw. der Kontrolle zur Einhaltung der

bestehenden Rechte gibt. Denn Aus oben genannten Gründen verstößt die App eindeutig gegen bestehendes deutsches Datenschutzrecht, ist aber noch immer in den betreffenden Stores zu erwerben, obwohl die Missstände bereits 2013 aufgedeckt wurden.

Zusammenfassend lässt sich sagen, dass zwar gesetzliche Regelungen zum Datenschutz bestehen, diese jedoch häufig missachtet oder umgangen werden. Der Digitale Wandel hat in relativ kurzer Zeit zu einem enormen Wachstum in technischen Bereichen geführt. Zum einen werden technische Geräte schnell leistungsfähiger, wodurch mehr Daten in digitaler Form gespeichert werden, zum anderen sorgt dieser Wandel dafür, dass immer mehr Bereiche des Lebens durch neue Technologien geregelt oder beeinflusst werden. Obwohl der Begriff des Datenschutzes bereits 1960 in Deutschland Anwendung fand, vollzog sich in den letzten Jahren ein Wandel des Begriffes hin zum Schutz von elektronischen Daten, nicht zuletzt bedingt durch die zunehmende Digitalisierung und die seltenere Verwendung Analoger Daten. Gerade durch die ständig neu entstehenden Möglichkeiten ist es schwer, das Datenschutzgesetz auf diese Veränderungen anzupassen.

4. Verwendung persönlicher Daten

Nachdem nun ein Überblick über die Entwicklung des Datenschutzes gegeben wurde, muss noch die Frage geklärt werden, was mit den Daten passiert – egal ob freiwillig zur Verfügung gestellt oder unfreiwillig gesammelt.

4.1 Internetkriminalität

Eine der meistbekannten Formen der Internetkriminalität ist das sogenannte Phishing. Dabei werden verschiedene Methoden wie zum Beispiel gefälschte Internetseiten, Emails oder Schadsoftware an den Benutzer gebracht, um so Zugang zu seinen persönlichen Daten zu erhalten. Vor allem bei der zunehmend genutzten Möglichkeit des Online-Bankings (Laut statistia.com etwa 57% der

deutschen Internetnutzer allein 2014) kann es hier zu erheblichen Schäden für den Betroffenen kommen. Durch die zunehmende Digitalisierung und die immer häufigere zentrale Speicherung von Daten, durch sogenanntes Cloud-Computing wie beispielsweise die ICloud von Apple, werden Daten auch anfälliger gegenüber Hacking-Angriffen. So wurde die ICloud 2014 Ziel eines Hacker-Angriffs, wobei viele private Daten wie Fotos und Telefonnummern von amerikanischen Prominenten ausgelesen und anschließend veröffentlicht wurden. Laut Apple wurde der Angriff durch verschiedene Software zum automatisierten ausprobieren von Passwörtern und Sicherheitsabfragen ermöglicht (Quelle http://www.sueddeutsche.de/digital/icloud-gehackt-aus-der-wolke-gefallen-1.2114705).

4.2 Big Data

Als Big Data werden gesammelte Datenmengen bezeichnet, die aufgrund ihrer Größe und Struktur nicht mehr mit den üblichen Methoden ausgewertet werden können. Zur Auswertung dieser Daten sind komplexere Algorithmen notwendig, welche verschiedenste Informationen gewinnen können. So werden diese Beispielsweise genutzt, um Suchanfragen und Verhalten von Nutzern auf Online-Märkten auszuwerten und so Werbung besser platzieren zu können oder Marktforschung zu betreiben.

Neben diesen von den Benutzern häufig kritisch betrachteten Verwendungen bietet Big Data aber auch ein großes Potential für verschiedene Einsatzgebiete. In den USA wird seit 2010 beispielsweise ein Programm der Polizei getestet, bei dem durch Big Data mögliche Orte für Verbrechen in der nächsten Zeit berechnet werden kann. Durch verstärkte Präsenz der Polizei an den berechneten Orten habe die Kriminalität dort bis zu 30% abgenommen (Quelle http://www.welt.de/vermischtes/article131982583/Die-Datenspur-des-vernetzten-Verbrechers.html). Auch in der Medizin wird über die Verwendung von Big Data diskutiert. So soll dadurch ein erweitertes Wissen zur Entstehung von Krankheiten, der Prävention und über individualisierten Therapien entstehen (Quelle http://www.aerzteblatt.de/archiv/147556/Datenanalyse-Big-Data-in-der-

Medizin). Ein Beispiel für die Anwendung in der Medizin zeigt der 2008 gestartete Dienst ‚Google Flue Trends'. Dieser Dienst sammelt Informationen über Suchbegriffe zu bestimmten Symptomen, Krankheiten oder Medizin und wertet diese anhand der zugehörigen IP-Adresse nach räumlicher Zugehörigkeit aus. Durch die Sammlung und Auswertung dieser Daten entsteht eine Landkarte die zeigt, in welchen Regionen Suchbegriffe zu bestimmten Krankheiten gehäuft vorkamen, also einem erhöhtem Aufkommen dieser Krankheit zu rechnen ist. Auch lassen sich aus den Daten Informationen über die Verbreitung von Krankheiten und die Entstehung von Epidemien gewinnen. (Quelle https://en.wikipedia.org/wiki/Google_Flu_Trends).

5. Fazit

In den letzten etwa 50 Jahren lässt sich in Deutschland ein gewisser Trend erkennen. Zum einen wurden vor allem in der ehemaligen BRD die Grundlagen für die Verankerung des Datenschutzes im Gesetz geschaffen. Durch die Entwicklung über das Hessische Datenschutzgesetz über das Bundesdatenschutzgesetz und deren regelmäßige Anpassung und Überarbeitung bis zur heutigen Zeit zeigt sich, dass sich die Anforderungen an die Gesetze schnell ändern. Im Zusammenhang mit dem technischen Fortschritt und der Digitalisierung in den letzten 10 bis 15 Jahren und der in diesem Zeitraum wachsenden Relevanz von Technik für den privaten Gebrauch entstanden zahlreiche Vorteile, die jedoch einer neuen Betrachtungsweise des Datenschutzes erfordern. Zum einen verwenden wir viele auch internationale Dienste, deren Datenschutzbestimmungen nicht immer mit deutschem Recht konform sind. Zum anderen werden vor allem durch die Digitalisierung unserer Daten viele Möglichkeiten geschaffen, auf diese – auch unerlaubt – zuzugreifen. Da die Digitalisierung in den vergangenen Jahren auch auf Bereiche des Onlinehandels oder des Bankings Auswirkungen hatte, wurden für Kriminelle auch lukrative Quellen geschaffen. Vor allem bei Big Data zeigt sich allerdings, dass unsere Daten auch die Möglichkeit haben in Bereichen wie Medizin oder der Kriminalitätsbekämpfung einen wichtigen Beitrag zu leisten.

Quellenverzeichnis

https://en.wikipedia.org/wiki/The_Right_to_Privacy_(article)

https://de.wikipedia.org/wiki/Datenschutz#Geschichte

https://de.wikipedia.org/wiki/Ministerium_f%C3%BCr_Staatssicherheit

Macrakis ‚Die Stasi-Geheimnisse: Methoden und Technik der DDR-Spionage'

https://de.wikipedia.org/wiki/BSP-12

https://de.wikipedia.org/wiki/Hessisches_Datenschutzgesetz

https://de.wikipedia.org/wiki/Hessischer_Datenschutzbeauftragter

https://de.wikipedia.org/wiki/Bundesbeauftragter_f%C3%BCr_den_Datenschutz_und_die_Informationsfreiheit

https://de.wikipedia.org/wiki/Bundesdatenschutzgesetz

https://de.wikipedia.org/wiki/Volksz%C3%A4hlungsurteil

https://de.wikipedia.org/wiki/Artikel-10-Gesetz

https://de.wikipedia.org/wiki/Digitale_Revolution

http://www.sciencemag.org/content/332/6025/60

http://www.golem.de/news/ieee-datenvolumen-im-internet-verdoppelt-sich-alle-zwei-jahre-1208-93957.html

https://de.wikipedia.org/wiki/Integrierter_Schaltkreis

https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/AusstattungGebrauchsguetern/Tabellen/Infotechnik_D.html

https://de.wikipedia.org/wiki/Andrej_Holm

http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-fuer-eine-0-006-Prozentpunkte-hoehere-Aufklaerungsquote-151466.html

http://www.gesetze-im-internet.de/gg/art_10.html

http://www.zeit.de/politik/deutschland/2015-06/vorratsdatenspeicherung-spd-sigmar-gabriel

https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/ITNutzung/Aktuell_ITNutzung.html

https://www.destatis.de/DE/Publikationen/WirtschaftStatistik/Informationsgesellschaft/ECommercePrivateHaushalte_82014.pdf?__blob=publicationFile

http://de.statista.com/themen/757/amazon/

http://de.statista.com/statistik/daten/studie/157490/umfrage/anzahl-der-auktionen-auf-ebay-in-ausgewaehlten-laendern/

http://www.haendlerbund.de/datenschutz

https://de.wikipedia.org/wiki/Web_Analytics

http://de.statista.com/statistik/daten/studie/70189/umfrage/nutzer-von-facebook-in-deutschland-seit-2009/

http://www.heise.de/newsticker/meldung/Datenschutz-bei-Facebook-USA-widersprechen-EuGH-Generalanwalt-wegen-Safe-Harbour-2831242.html

http://de.statista.com/statistik/daten/studie/197383/umfrage/mobile-internetnutzung-ueber-handy-in-deutschland/

https://play.google.com/store/apps/details?id=goldenshorestechnologies.brightestflashlight.free

http://www.giga.de/apps/google-play-store/news/taschenlampen-app-verkauft-ungefragt-daten-von-millionen-nutzern/

http://www.sueddeutsche.de/digital/icloud-gehackt-aus-der-wolke-gefallen-1.2114705

http://www.welt.de/vermischtes/article131982583/Die-Datenspur-des-vernetzten-Verbrechers.html

http://www.aerzteblatt.de/archiv/147556/Datenanalyse-Big-Data-in-der-Medizin

https://en.wikipedia.org/wiki/Google_Flu_Trends