Von Goldstandards und sicheren Häfen

Datenschutz zwischen EU und USA

Jan Alexander Linxweiler

Das Thema Datenschutz stellt schon allgemein eine Kontroverse dar. Das Zusammenspiel von Regulierungen und Freiheit dominiert die innerstaatlichen oder auch supranationalen Diskussionen. Wenn man jedoch das Blickfeld weitet und somit auch den Diskussionsrahmen, wird eine ganz neue Dimension eröffnet. Im Hinblick auf die europäische Datenschutzverordnung strandet man dann sofort an der US-amerikanischen Küste. Dort wird unter Verweis auf das *Safe Harbor Agreement* scharfe Kritik an den Entwürfen der EU-Justizkommissarin Viviane Reding laut und dabei deutlich, wie sehr die europäischen und amerikanischen Vorstellungen von Datenschutz divergieren.

Systeme und Traditionen – Unterschiede zwischen der EU und den USA

Die Ursprünge des Datenschutzes lassen sich in den verschiedenen Facetten mehr als 100 Jahre zurückdatieren. Das Recht „to be let alone", welches bereits 1890 von *Warren* und *Brandeis* in ihrer bahnbrechenden Schrift „The Right to Privacy" vertreten wurde, korrelierte schon in diesen Überlegungen mit wachsenden technischen Errungenschaften.[1] So entwickelten sich über die Zeit verschiedene Modelle zum Datenschutz, von denen sich heute im Speziellen vier hervorheben. Der Schutz durch umfassende Gesetze („comprehensive laws") schafft einen Gesetzesrahmen für das Sammeln, Nutzen und die Verbreitung persönlicher Informationen, der durch offizielle Behörden überwacht und durchgesetzt werden soll. Es handelt sich hierbei um einen eher proaktiven Ansatz zum Datenschutz. Dem gegenüber stellt der Schutz durch sektorale Gesetze („sectoral laws") einen reaktiven Ansatz dar, der sich mit spezifischen und konkreten Einzelbereichen und -problemen des Datenschutzes befasst. Der Schutz durch wirtschaftliche Selbstregulierung („industrial self-regulation") ist der wohl flexibelsten Ansatz, verlässt sich dabei allerdings lediglich auf die selbst auferlegten Regeln der Wirtschaftsteilnehmer. Letztlich gibt es noch den Schutz durch Privatsphäre schützende Technologien („privacy-enhancing technologies"), die vor allem Verschlüsselungstechnologien, digitale Währungen und ähnliches umfassen.[2]

Die Umsetzung in den einzelnen Staaten erfolgt nun in unterschiedlichsten Formen und Variationen, aber zumeist durch die Kombination dieser Modelle. Wie wiederum die Kombination erfolgt, hängt vor allem von der Auffassung und Bewertung des Datenschutzes an sich ab. In der Kontrastierung der EU und der USA kann man zwei vollkommen gegensätzliche Ansätze beobachten. In den USA wird traditionell ein eher liberalerer Datenschutz-Ansatz verfolgt. Wahrgenommen wird hier ein Gefahrenpotential, das eher vom Staat als vom privaten Sektor ausgeht. Der Datenschutz ist hier die Manifestation eines individuellen Eigentumsrechts, über welches nach bestem Gewissen aber auch Gutdünken verfügt werden kann. Einschränkungen findet dies, nach einer Entscheidung des Supreme Court, nur in einem limitierten Rahmen hinsichtlich des Schutzes vor staatlicher Überwachung.[3] Ferner steht der Datenschutz im starken Konflikt mit der Rede- und Pressefreiheit, welche durch den ersten Verfassungszusatz garantiert wird. Folge ist, dass Vorstöße der EU – vor allem das „Right to be forgotten" – Friktionen mit der bestehenden Rechtsprechung hervorrufen.[4] Die USA verlassen sich hierbei auf eine Vielzahl von staatlichen und föderalen Statuten und Doktrinen, mithin also sektorale Gesetzgebung. Hierzu zählen unter anderem der „Intelligence Surveillance Act", der „Children Online Privacy Protection Act", der "Protect IP Act" und der „Health Insurance Portability and Accountability Act". Schon allein aus den Namen wird ersichtlich, wie fragmentarisch und reaktiv die Ausgestaltung des Datenschutznetzwerkes ist. Ferner ist zu beobachten, dass der Datenschutz primär nur an den Verbraucherschutz und das Wettbewerbsrecht anknüpft. Hinzu kommt die Abwesenheit einer überwachenden Durchsetzungsbehörde. Vielmehr wird auf ein starkes selbstregulatorisches Element gesetzt, welches Raum für Leistungspotential und Flexibilität in einem sich schnell wandelnden Medium wie dem Internet bieten soll.[5] So ermangelt es beispielsweise der Federal Trade Commission (FTC) an effektiven Durchsetzungsmechanismen im Datenschutz-Bereich, da sie auf die Mitarbeit der Unternehmen selbst angewiesen ist.

1 *Warren/Brandeis*, 'The Right to Privacy', Harvard Law Review, No. 4, 1890, S. 2f.

2 *Long/Pang Quek*, Personal data privacy protection in an age of globalization: The US-EU safe harbor compromise, Journal of European Public Policy, 9:3, S. 325-344.

3 Katz v. United States, 386 U.S. 954, 1967.

4 *Bennett*, The „Right To Be Forgotten": Reconciling EU and US perspectives, Berkeley Journal of Internat'l Law, 2012, S. 4f.

5 *Long/Pang Quek* (Rn. 2), S. 332f.; *Korbin*, Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance, Review of International Studies (2004), 30, 115.

Demgegenüber ist die Datenschutztradition der EU im Grundgedanken der Supranationalität verwurzelt.[6] Der Schwerpunkt liegt hier auf der Uniformität des Datenschutzes innerhalb Europas, um Barrieren zwischen den Mitgliedsstaaten sowie aus solchen erwachsende Ungleichbehandlungen abzubauen. Ziel ist ein Datenschutz, der die weitest mögliche Akzeptanz unter den Mitgliedern erlangt, indem die Essentialia der nationalen Datenschutz-Lösungen in einem uniformen Gesetz vereint werden.[7] Ferner wird der Schutz des Individuums gegenüber der Wirtschaft fokussiert und die Bürde des Schutzes der Staatengemeinschaft auferlegt.[8] Dieser Gesetzesrahmen stellt – wie erwähnt – einen eher proaktiven Ansatz dar, wobei selbiger im Bezug auf außereuropäische Datenschutz-Regime durch ein reaktives Element ergänzt wird. Artikel 25 der EU-Datenschutzrichtlinie (RL 95/46/EG) verpflichtet die EU nämlich in solchen Fällen zu einer Einzelfallanalyse, wenn die persönlichen Daten von EU-Bürgern betroffen sind.[9] Ferner soll nach dem vorliegenden Entwurf einer Datenschutzverordnung eine Durchsetzungsbehörde innerhalb des Unionssystems installiert werden.

Genau dieser Ansatz der EU verschärft den Konflikt zwischen den beiden grundsätzlich verschiedenen Ansätzen noch weiter. Denn es wird damit auch ein Streit über den Zuständigkeitsbereich („Jurisdiction") aufgeworfen.[10] Nach klassischer Völkerrechtslehre wird die Zuständigkeit der Gerichtsbarkeit durch die Souveränität eines Staates festgestellt. Es soll sichergegangen werden, dass die Unabhängigkeit und Gleichheit der interagierenden Souveräne beibehalten wird.[11] Auch hier divergieren die Ansichten der USA und der EU bezüglich des Anknüpfungspunktes der Zuständigkeit. Die USA machen es – nach der so genannten „Zippo-Entscheidung" – innerhalb einer Einzelfallbetrachtung davon abhängig, ob tatsächlich eine wirtschaftliche Transaktion stattgefunden hat oder lediglich Informationen ausgetauscht wurden.[12] Im Gegensatz dazu sieht sich die EU – wie bereits oben erwähnt – in all den Fällen zuständig in denen Daten von EU-Bürgern gesammelt werden oder auf solche zugegriffen wird.[13]

„Neuer Goldstandard" anstatt „sicherer Häfen" - die europäische Datenschutzverordnung im Prozess

Der erste Ansatz zur Lösung des beschriebenen Konflikts war das so genannte *Safe Harbor Agreement*, welches zwischen 1998 und 2000 entwickelt wurde.[14] Diese Datenschutzvereinbarung sollte den Datenverkehr zwischen EU und USA im Einklang mit der Richtlinie 95/46/EG (Datenschutzrichtlinie) regeln.[15] Ziel war dabei die Balance zwischen dem nach europäischer Ansicht adäquaten Datenschutz und der durch die USA präferierten Selbstregulation des Marktes.[16] In den USA würde danach ein „sicherer Hafen" für Unternehmen geschaffen, indem diese sich den Vorgaben der „Safe Harbor Privacy Principles" unterwerfen konnten.[17] Diese umfassen folgende Regelungen:

Einzelpersonen müssen darüber in Kenntnis gesetzt werden, dass ihre Daten gesammelt und genutzt werden.

Einzelpersonen muss die Möglichkeit zugestanden werden, sich aus der Sammlung, Nutzung und Weitergabe ihrer Daten auszuklinken („opt-out").

Die Weitergabe von Daten an Dritte darf nur dann erfolgen, wenn diese denselben, adäquaten Datenschutzstandard innehaben.

Es müssen angemessene Maßnahmen zur Sicherung der gesammelten Daten getroffen werden.

Die Daten müssen überhaupt relevant für den Datensammlungsprozess selbst sein.

Einzelpersonen müssen Zugriff auf die von ihnen gesammelten Daten haben und diese im Falle der Unrichtigkeit auch löschen können.

Es müssen effektive Durchsetzungsmechanismen vorliegen.

Jedoch unterwerfen sich die Unternehmen lediglich auf freiwilliger Basis. Das *Department of Commerce* zertifiziert dabei jährlich die Einhaltung von selbstregulierenden Programmen, die dem „Safe Harbor Privacy Principles" entsprechen. Es ist auch das *Department of Commerce*, welches 2007 das *Safe Harbor Agreement* als „Gold Standard for data protection" proklamierte. Auf der europäischen Seite wurde eine Implementierung durch einen Artikel vollzogen, der diese „Principles" als ausreichend akzeptiert. Mithin stellt das *Safe Harbor Agreement* in keinem Fall ein internationales Abkommen im technischen Sinne, sondern lediglich die Summe einzelner unilateraler Akte dar.[18]

Letztlich überzeugte diese Vorgehensweise jedoch die Fraktionen auf beiden Seiten des Atlantiks nicht. Dies gilt gerade vor dem Hintergrund, dass in den regelmäßigen Überprüfungen gravierende Mängel festgestellt wurden. Diese umfassen verschiedenste Punkte von Transparenz bis Akkuratesse. So waren im Jahre 2008 von 1597 gelisteten Organisationen nur 1109 noch zertifiziert oder überhaupt noch existent. Ferner erreichten nur 348 davon den Mindeststandard der aufgeführten „Principles". Hierbei bestanden die größten Defizite im Bereich Durchsetzung und Konfliktlösungsmechanismen. Außerdem wurden im selben Überprüfungszeitraum 206 Organisationen ermittelt, die fälschlicherweise behaupteten, dass sie Mitglieder im Safe Harbor Agreement seien; manche fälschten sogar

6 Vgl. *Reding*, Rede Washington/Brüssel, 19 März 2012, „Towards a new „Gold Standard" in Data Protection?", http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/20120319speech-data-gold-standard_en.pdf (zuletzt besucht am 27.08.2012).
7 *Simitis*, (1998) zitiert in Long/Pang Quek (Fn 2), S. 333..
8 *Korbin* (Fn. 5), S. 116.
9 *Long/Pang Quek* (Fn. 2), S. 334.
10 *Korbin* (Fn. 5), S. 111–131.
11 *Hobe*, Einführung in das Völkerrecht, S. 37.
12 *Bennett* (Fn. 4), S. 5.
13 *Long/Pang Quek* (Fn. 2), Seite 334; *Bennett*, (Fn 4), S. 5.
14 http://export.gov/safeharbor/eu/eg_main_018493.asp (zuletzt besucht am 09.09.2012)
15 *Connolly*, The US Safe Harbor – Fact or Fiction?, 2008, Galexia, S. 4.
16 *Korbin* (Fn. 5), S. 120.
17 *Long/Pang Quek* (Fn. 2), S. 336.
18 *Korbin* (Fn. 5), S. 121.

Prüfzeichen.[19]

In den USA selbst wird das Übereinkommen ebenfalls kritisch beäugt. Vor allem die kostspieligen Defizite in den gerade genannten Bereichen, aber auch der grundsätzliche Druck, den es auf die Legislative ausüben könnte, ruft vor dem Hintergrund der amerikanischen Datenschutz-Tradition Misstrauen hervor. Allerdings gibt es auch Fraktionen in den USA, die in gegenteiliger Hinsicht besorgt sind: Nämlich, dass das Übereinkommen nicht weitläufig und tiefgreifend genug ist.[20]

Die EU auf der anderen Seite stand dem Unterfangen von Beginn an mit Skepsis gegenüber. Befürchtungen, dass die Adäquanz des Art. 25 der Datenschutzrichtlinie durch das Safe Harbor Agreement nicht gewährleistet sei, wurden durch besagte Überprüfungen bestätigt.[21] Der angestrebte Datenschutz für die EU-Bürger konnte nicht sichergestellt werden, sodass ein erneutes Angehen der Thematik notwendig erschien.[22]

Aus diesem Ansinnen entstand dann der Entwurf der neuen Datenschutz-Verordnung. Die nahezu unmittelbar folgende Kritik der USA an diesem Entwurf bewegt sich dabei beinahe symptomatisch in den traditionell-verwurzelten Argumentationsbahnen. Im Fokus steht vor allem die kommerzielle Interoperabilität, welche durch den Entwurf als behindernd und für Konsumenten sogar kontraproduktiv angesehen wird. Die FTC erklärt nachdrücklich, dass eine (Über)Regulierung, wie sie im vorliegenden Entwurf zu erkennen wäre, eher zu Divergenzen als zu Konvergenz führen könnte. Hierbei werden alternativ die Verhaltensregeln des Safe Harbor Agreement gerühmt und die Meldepflicht von Verletzungen der Datensicherheit kritisiert. Eine solche Meldepflicht, die unabhängig vom Umfang und Gewichtung des Vorfalles bestehe, sei zu umfänglich. Fortführend werden negative Auswirkungen auf die Redefreiheit sowie weitere Menschenrechte befürchtet. Dabei steht insbesondere das „Recht auf Vergessen" („the right to be forgotten") im Mittelpunkt. Es wird sowohl dessen enge Ausgestaltung in Art. 80 DSGVO-E kritisiert, als auch dessen technische Umsetzbarkeit in Frage gestellt. Zusätzlich sei auch die internationale Zusammenarbeit im Bereich der Strafverfolgung und die Interoperabilität von Regulierungsbehörden gefährdet. Eine Anmeldung und Autorisierung von Maßnahmen bei europäischen Datenschutzbehörden sei nicht nur umständlich, sondern geradezu widersprüchlich zur effektiven Durchführung selbiger Maßnahmen. Letztlich könnte, so die Ansicht der US-Vertretung, auch die Zivilgerichtsbarkeit mit Problemen zu kämpfen haben.[23]

Auf diese durchaus harsche und umfangreiche Kritik reagierte die EU mit Beharren auf den zentralen Punkten des Entwurfes. So wird stets betont, dass der Dreh- und Angelpunkt eines Datenschutzrechtes im Vertrauen der Verbraucher auf Sicherheit und Schutz beruhe. Ein solches Regime könne nur bestehen bleiben, wenn es sich weiterentwickele und an technischen Wandel und Notwendigkeiten anpasse.[24] Ferner wird auch Emphase auf die Notwendigkeit von Durchsetzungsbehörden und -mechanismen gelegt.[25] Zusammenfassend kann gesagt werden, dass die EU von ihrem Ansatz im Bereich des „comprehensive law" nicht abrückt, sondern vielmehr die USA auffordert, mitwirkend tätig zu werden. So wird auch wiederholend die Consumer Privacy Bill of Rights der Obama Administration lobend hervorgehoben. Diese Bestrebungen der Zusammenarbeit verbalisiert die EU-Justizkommissarin Viviane Reding auf der EU-Konferenz zum Thema „Privatsphäre und Schutz von persönlichen Daten" mit folgendem Zitat treffend:

„Let us build together a new gold standard of data protection based on clear and strong laws that will allow our businesses and citizens to fully benefit from the digital economy."[26]

Die Küste vor Augen – Blick in die Zukunft des Datenschutzes

In conclusio bleibt zu hoffen, dass die europäische Datenschutzverordnung einen Anstoß für eine internationale und nicht allein supranationale Lösung der Datenschutzproblematik sein kann. Der von Viviane Reding angestrebte „New Gold Standard in Data Protection" könnte und muss auch eine solide Lösung für den internationalen Datenaustausch unter Berücksichtigung der Bedürfnisse und Traditionen der (wirtschaftlichen) Großmächte USA und EU darstellen. Probleme der Interoperabilität und des Rechtsschutzes können nur auf einer kooperativen Basis nachhaltig geklärt werden. Letztlich birgt nämlich das Safe Harbor Agreement kein nachhaltiges Versprechen auf Lösung des Ungleichgewichts und der Divergenz in den verschiedenen Datenschutzregimen.

19 *Connolly* (Fn. 14), S. 4 ff.

20 *Korbin* (Fn. 5), S. 122.

21 *Ibid.*

22 *Long/Pang Quek* (Fn. 2), S. 338.

23 Informelle Note der U.S. Federal Trade Commission, http://www.statewatch.org/news/2012/jan/eu-dp-usa-note.pdf.

24 Vgl. *Reding*, Rede London, 01. März 2012, „The importance of strong data protection rules for growth and competitiveness", http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/171&format=HTML&aged=0&language=EN&guiLanguage=en (zuletzt besucht am 27.08.2012).

25 Vgl. *Reding*, Rede Luxemburg, 03. Mai 2012, „Strong and indipendent data protection authoritis: the bedrock of the EU's data protection reform", http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/316&format=HTML&aged=0&language=EN&guiLanguage=en (zuletzt besucht am 27.08.2012).

26 *Reding*, Rede Washington/Brüssel, 19 März 2012, „Towards a new „Gold Standard" in Data Protection?", http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/20120319speech-data-gold-standard_en.pdf (zuletzt besucht am 27.08.2012).