



# Jugendsession 2015

27. – 30. August 2015

**> Dossier**

**Datenschutz**

## Inhalt

1. Datenschutz – was ist das?.....	3
2. Datensammlung.....	4
2.1 Von was für Daten sprechen wir im Zusammenhang mit dem Datenschutz?.	4
2.2 Datensammlung im grossen Stil .....	4
2.3 Wer hat ein Interesse an deinen Daten? .....	5
3. Datenschutz in der Schweiz.....	7
3.1 Wie und wo ist der Datenschutz in unserem Gesetz geregelt? .....	7
3.2 Datenschutz- und Öffentlichkeitsbeauftragter .....	8
4. Einblick in den politischen Diskurs in der Schweiz.....	9
4.1 Revision des Datenschutzgesetzes .....	9
4.2 Zwei umstrittene Gesetzesvorlagen .....	10
4.2.1 BÜPF.....	11
4.2.2 Nachrichtendienstgesetz .....	12
5. Datenschutz – eine globale Herausforderung .....	13
6. Datenschutz und Eigenverantwortung .....	14
7. Weitere Informationen.....	16

## 1. Datenschutz – was ist das?

Unsere globalisierte Welt ist ohne einen ständigen Datenaustausch kaum noch vorstellbar. Ob in der Wirtschaft, beim Staat oder auch in deiner privaten Kommunikation – überall werden ständig Daten ausgetauscht und gespeichert. Dieser permanente Austausch ist für unsere heutige Welt unabdingbar und auch dein Alltag ist stark von diesem Datenverkehr geprägt. Täglich gibst du persönliche Daten von dir preis – oft unbewusst.

Diese persönlichen Daten – Personendaten genannt – sind ein wertvolles Gut. Insbesondere Unternehmen haben ein grosses Interesse an diesen Daten. Millionenfach werden sie gesammelt, um z.B. das Konsumverhalten zu erforschen oder gezielt Werbung zu schalten. Nicht selten werden solche Daten auch gehandelt. Ausserdem sind diese Daten für den Staat sehr interessant. Denke z.B. an den Kampf gegen den Terrorismus oder die Kriminalität.

Immer wenn Personendaten als blosses Wirtschaftsgut oder Ressource/Mittel für irgendeinen Zweck angesehen werden, spricht man vom materiellen Wert von Personendaten.

Dabei wird aber ein ganz zentraler Aspekt von Personendaten ausgeblendet. Personendaten sind immer mit einer Person verknüpft. Diese Person kann der Information einen ganz subjektiven Wert zuordnen (ideeller Wert von Personendaten). So kann z.B. die Info über dein Alter oder deine Religionszugehörigkeit für dich einen hohen Wert haben und du willst nicht, dass die ganze Welt auf diese Daten zugreifen kann.

Personendaten dürfen deshalb nicht nur auf ihre materielle Dimension beschränkt werden. Der Austausch und die Speicherung solcher Daten sollte auf den persönlichen Wert der betreffenden Person Rücksicht nehmen. In unserer demokratischen Gesellschaftsordnung gilt: **Jeder Mensch soll so weit wie nur möglich selber darüber bestimmen können, welche Informationen über ihn wann, wo und wem bekannt gegeben werden. Damit dieser Grundsatz eingehalten wird, gibt es den Datenschutz.**<sup>1</sup>

Es geht somit beim Datenschutz nicht um den Schutz von Daten, wie man es fälschlicherweise verstehen könnte, sondern vielmehr um den Schutz der Personen, die hinter solchen Daten stecken. Die informelle Selbstbestimmung ist dabei ein Grundsatz: du sollst soweit wie möglich selbst darüber bestimmen, was mit deinen persönlichen Daten passiert.

Die Bundeszentrale für politische Bildung definiert Datenschutz wie folgt:

*Datenschutz ist die Gesamtheit von Regeln, Institutionen und Massnahmen, um die informationelle Selbstbestimmung der Bürger zu schützen. Er schützt nicht die Daten (des Datenbesitzers), sondern den von Datenverarbeitung "Betroffenen" (gegen den Datenverarbeiter).*<sup>2</sup>

---

<sup>1</sup> <http://www.edoeb.admin.ch/datenschutz>

<sup>2</sup> <http://www.bpb.de/40258/datenschut>

## 2. Datensammlung

### 2.1 Von was für Daten sprechen wir im Zusammenhang mit dem Datenschutz?

Wie bereits erläutert geht es um personenbezogene Daten. Das Schweizer Gesetz verwendet hierfür den Begriff Personendaten. Doch was fällt alles unter den Begriff Personendaten?

Einerseits sind dies die klassischen persönlichen Angaben wie: Name, Geburtsdatum, Augenfarbe, Geschlecht, Religion usw. Dazu kommen jedoch auch sachliche Angaben wie: Autokennzeichen, AHV-Nummer oder Vermögensverhältnisse. Verkürzt kann man sagen, dass alle Informationen, welche sich einer bestimmten Person zu ordnen lassen, als Personendaten gelten und somit unter Datenschutz stehen. In der Schweiz ist speziell, dass der Begriff Person, neben der natürlichen Person (Fachbegriff aus dem Recht für alle Menschen) auch die juristische Person (Firmen etc.) einschliesst.

Weiter gibt es den Ausdruck *Besondere Personendaten*. Das sind diejenigen Personendaten, bei deren Bearbeitung die Gefahr von Persönlichkeitsverletzungen besonders gross ist. Hier ist ein guter Datenschutz wichtig. Dazu zählen laut Schweizer Gesetz insbesondere Angaben zu folgenden Themenbereichen<sup>3</sup>:

- religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten;
- Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit;
- Massnahmen der sozialen Hilfe;
- administrative oder strafrechtliche Verfolgungen und Sanktionen.

### 2.2 Datensammlung im grossen Stil

Seine Anfänge nahm der moderne Datenschutz in den frühen 60er Jahren. Die rasante Entwicklung der Computertechnik machte es möglich, dass erstmals grosse Datenmengen elektronisch erfasst und gespeichert werden konnten. Die amerikanische Regierung unter John F. Kennedy wollte in dieser Zeit eine EDV (Elektronische Datenverarbeitung) Datenbank aufbauen, in der alle amerikanischen Staatsbürger erfasst werden sollten. Die Pläne stiessen jedoch in der Bevölkerung auf heftigen Widerstand. Eine öffentliche Debatte über die Privatsphäre entflammte, welche auch auf Europa überschwappte.<sup>4</sup> Das Ergebnis der öffentlichen Diskussionen in den USA war, dass die Datenbank nicht errichtet und stattdessen der „Privacy Act“ (Privatsphärengesetz) verabschiedet wurde - allerdings erst im Jahre 1974. Bereits vier Jahre zuvor wurde im deutschen Bundesland Hessen das erste Datenschutzgesetz der Welt verabschiedet.

1989 deckte eine parlamentarische Untersuchungskommission auf, dass die Bundesanwaltschaft der Schweiz Hunderttausende politisch aktive Bürger überwacht hatte. 900'000 sogenannter Staatsschutz-Fichen wurden zwischen 1900

---

<sup>3</sup> <https://www.admin.ch/opc/de/classified-compilation>

<sup>4</sup> <http://suite101.de/article/geschichtliches-zum-datenschutz-a50488#.VadiVjop-DQ>

und 1990 zum Zwecke des Staatschutzes angelegt.<sup>5</sup> Ganze Archive voller Karteikarten mit persönlichen Daten haben sich angesammelt. Die Aufdeckung dieser „Schnüfflerei“ ging als Fichen-Affäre in die Geschichte der Schweiz ein und erschütterte die gesamte Bevölkerung. 1992 lancierte die Schweiz das Bundesgesetz über den Datenschutz (DSG), welches bis heute Bestand hält.

Mit der Digitalen Revolution um die Jahrtausendwende herum, veränderte sich unsere Welt gewaltig. Leistungsstarke Mikrochips, hochtechnisierte Computersysteme und nicht zu letzt das Internet bewirkten einen Wandel in fast allen Lebensbereichen. In den letzten Jahren ist das Internet und die Menge an digitalen Daten wortwörtlich explodiert. Heute werden in 10 Minuten quantitativ betrachtet mehr Daten erstellt und gesammelt als in all den Jahren der Menschheitsgeschichte vor dem 21. Jahrhundert zusammen<sup>6</sup>. Die Zukunft gehört Big Data – der Bearbeitung riesiger Datenmengen, welche jegliche Vorstellungskraft sprengen - eine Entwicklung, die den Datenschutz vor gewaltige Herausforderungen stellt.

### 2.3 Wer hat ein Interesse an deinen Daten?

Die beiden Hauptakteure im Sammeln von Personendaten sind der Staat (die öffentliche Hand) sowie Unternehmen (Privatwirtschaft). Natürlich kann heute jeder Daten sammeln. Im Internet wimmelt es von Personendaten, auf welche alle ganz einfach zu greifen können. Mit Smartphones, Drohnenkameras und all den anderen Gadgets die es heute gibt, können auch direkt Personendaten (Bilder, Videos etc.) gesammelt werden. Du kannst somit nie sicher sein, ob du nicht gerade gefilmt wirst und das Video wenig später auf Youtube landet. Privatpersonen können heute Daten ohne Probleme sammeln und diese auch missbrauchen. Bereits mit Grundlagenwissen im Hacking können Einzelpersonen gigantische Datenmengen „stehlen“.

Für das Funktionieren der modernen öffentlichen Verwaltung / Staates sind Datensammlungen unerlässlich: Das Handelsregister, der Energieverbrauch, Einkommen oder Unfallstatistiken - überall werden Daten erfasst, gespeichert und ausgewertet. Die meisten Daten werden dabei anonymisiert, das heisst es ist keine Verknüpfung zu einer Person mehr vorhanden und somit steht dies in keinem Konflikt zum Datenschutz.<sup>7</sup> Dennoch werden auch viele Daten gesammelt, die personenbezogen sind. Der Staat muss diese teilweise tun, um sein Funktionieren zu gewährleisten, denke z.B. an Steuerdaten. Mit solchen Daten muss dann jedoch äusserst sensibel umgegangen werden und sie dürfen nicht veröffentlicht werden. Doch es gibt auch personenbezogene Daten, deren Veröffentlichung als legitim erscheinen kann, z.B. im Kampf gegen Terrorismus und Kriminalität. Ein strikter Datenschutz kann als Versteck für Kriminelle missbraucht werden und bei Ermittlungen der Polizei hinderlich sein. Wie die Schweiz diesen Grat zwischen

---

<sup>5</sup> <http://www.nzz.ch/die-seltsame-hinterlassenschaft-des-helvetischen-staatsschutzes-1.3015643>

<sup>6</sup> [www.bigdatablog.de/2015/05/03/](http://www.bigdatablog.de/2015/05/03/)

<sup>7</sup> «Einstein» vom 2.10.2014, Big Data

Datenschutz des Einzelnen und Transparenz im öffentlichen Interesse meistert, wird im nächsten Kapitel thematisiert.

Datensammlungen sind auch für viele Unternehmungen sehr Interessant. Mit Personendaten lässt sich Geld machen - und zwar ziemlich viel. Bestes Beispiel ist Facebook, mit einem geschätzten Wert von 50 Milliarden US-Dollar<sup>8</sup> - alles nur dank Personendaten. Doch was macht diese Daten so interessant und wertvoll für Firmen? Es ist vor allem der Werbesektor, welcher sich um diese Daten reisst.<sup>9</sup> Und Werbung ist ein essentieller Bestandteil jeder erfolgreichen unternehmerischen Tätigkeit. Wenn eine Firma eine Kontaktinfo von dir besitzt (z.B. E-Mail) und dann noch weiss, was du magst und wo du wohnst, kann sie dir - auf dich zugeschnittene - Werbung zustellen. Die Wahrscheinlichkeit, dass solch eine Werbung Wirkung zeigt ist dann sehr hoch. Wenn du bei Google den Begriff Pfanne eingibst, weiss Google, dass du ziemlich sicher eine Pfanne erwerben möchtest. Diese Info kann Google dann an einen Pfannenhersteller verkaufen.

Für Krankenversicherungen sind Gesundheitsdaten sehr interessant. Das Ziel jeder privaten Krankenversicherung ist es, möglichst viele junge und gesunde Kunden zu haben. Diese bezahlen fleissig ihre Prämien und beanspruchen keine/wenig Leistung. So ist zum Beispiel eine Teilnehmerliste eines Marathons für eine Krankenversicherung äusserst interessant.<sup>10</sup>

Gezielte Werbung sowie der Kontakt zu potentiellen Kunden sind durch den Erwerb von Personendaten möglich und machen diese Daten so wertvoll. Der Datenschutz erschwert jedoch den Zugang zu diesen Daten und ist deshalb einigen Firmen ein Dorn im Auge.<sup>11</sup>

Zusammenfassend gibt es somit drei Interessen, welche der Datenschutz berücksichtigen muss: Zum einen will die Person, welche mit den Daten in Verbindung steht, die Herrschaft über diese haben. Der Staat hat jedoch ein Interesse an der Verwendung dieser Daten, um seine Aufgaben effizient erfüllen zu können. Und schliesslich gibt es noch Private (Unternehmen etc.) welche mit Personendaten wirtschaftliche Interessen verfolgen.<sup>12</sup>

---

<sup>8</sup> [http://www.forbes.com/fdc/welcome\\_mjx.shtml](http://www.forbes.com/fdc/welcome_mjx.shtml)

<sup>9</sup> <http://www.n-tv.de/technik/So-fesselt-man-die-Facebook-Datenkrake-article14237491.html>

<sup>10</sup> ln-online.de, 16.07.2015 11:31 Uhr

<sup>11</sup> NZZ Online; 1.4.2015, 16:31 Uhr

<sup>12</sup> [www.it-recht.ch/wp-content/uploads/2014/11/Folien-Straub-Einfuehrung-ins-Datenschutzrecht-Uni-FR-06.12.2004.pdf](http://www.it-recht.ch/wp-content/uploads/2014/11/Folien-Straub-Einfuehrung-ins-Datenschutzrecht-Uni-FR-06.12.2004.pdf)

### 3. Datenschutz in der Schweiz

#### 3.1 Wie und wo ist der Datenschutz in unserem Gesetz geregelt?

Im Art. 13 der Bundesverfassung steht, dass jede Person Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehr sowie auf Schutz vor Missbrauch ihrer persönlichen Daten hat. Mit diesem Artikel gibt die Verfassung allen BürgerInnen das Recht auf Privatsphäre!

Um diesen Schutz auch in Zeiten der elektronischen Datenerfassung zu gewähren, wurde das Bundesgesetz über den Datenschutz (DSG) verabschiedet und ist seit dem 1. Juli 1993 in Kraft. Die entsprechende Verordnung (VDSG) regelt die Einzelheiten.

Die folgenden sieben Prinzipien können als Grundlage des DSG bezeichnet werden.

#### Die Grundsätze des Datenschutzes in der Schweiz:

- **Legalität, Gesetzmässigkeit:** Die Bearbeitung der Daten muss den allgemeinen gesetzlichen Rahmen einhalten.
- **Verhältnismässigkeit:** die Datensammlung muss in einen gesunden Verhältnis zum Zweck stehen
- **Zweckbindung:** Personendaten dürfen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben worden sind.
- **Daten-Richtigkeit:** die Daten müssen korrekt / aktuell sein
- **Transparenz** gegenüber den betroffenen Personen: Die Betroffenen müssen über Verwendung und Zweck der Daten informiert sein.
- **Informationssicherheit:** die Daten müssen sicher bearbeitet werden, sodass sie nicht an Dritte gelangen
- **Treu und Glauben:** dies ist ein allgemeines Prinzip, vor allem in der öffentlichen Verwaltung der Schweiz (Es bezeichnet das Verhalten eines aufrechten und anständig handelnden Menschen.<sup>13</sup>)

Wer Personendaten bearbeitet, das beinhaltet jeglichen Umgang mit Personendaten, muss sich an diese sieben Grundprinzipien halten. Nicht zu vergessen ist die informelle Selbstbestimmung, welche das Fundament des gesamten Gesetzes darstellt.

Viele dieser Prinzipien finden sich in Datenschutzgesetzen auf der ganzen Welt – vor allem in den westlichen Ländern<sup>14</sup>. Es gibt jedoch auch essenzielle Unterschiede.

In der Schweiz ist das Bearbeiten von Personendaten grundsätzlich erlaubt, erst wenn die Prinzipien und die daraus abgeleiteten Gesetze verletzt werden, wird dies illegal. Deutschland hingegen geht den gegenteiligen Weg. Bei unserem Nachbar und auch im EU-Recht gilt ein Verbot mit Erlaubnisvorbehalt. Dies besagt, dass das Bearbeiten von personenbezogenen Daten grundsätzlich verboten ist. Nur wenn ein

<sup>13</sup> <http://www.jurawelt.com/studenten/skripten/zivr/7246>

<sup>14</sup> <http://www.bpb.de/40258/datenschutz?p=0>



Beispiel, wie über die Verwendung von Daten informiert wird

im Gesetz verankerter Erlaubnisgrund zutrifft, ist die Datenerhebung/Bearbeitung legal.

In der Schweiz gilt die Auskunftspflicht. Wenn ich z.B. beim Bund Infos über meine gespeicherten Daten verlange, muss er mir diese aushändigen. Des Weiteren gibt es in der Schweiz eine Informationspflicht, was Deutschland nicht hat. Diese besagt, dass jeder der Personendaten sammelt und bearbeitet, die Inhaber dieser Daten informieren muss.

Wichtig anzufügen ist, dass die Bestimmungen des DSG für die Bundesbehörden sowie den gesamten privaten Raum gelten. Kantonale Behörden unterstehen jedoch dem jeweiligen kantonalen Datenschutz.

### 3.2 Datenschutz- und Öffentlichkeitsbeauftragter

Was sind die Aufgaben des EDÖB im Bereich des Datenschutzes?

Die Stelle des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) wurde geschaffen mit dem Zweck, Privatpersonen und Bundesorgane in Hinblick auf die Einhaltung der gesetzlichen Datenschutzbestimmungen zu beraten und zu beaufsichtigen. Das heisst, dass der EDÖB einerseits dazu beiträgt, die Personen, die Personendaten bearbeiten (also die Inhaber von Datensammlungen), aber auch die Personen, über die Daten bearbeitet werden (also die betroffenen Personen) für Aspekte des Datenschutzes zu sensibilisieren und sie zu informieren.

Andererseits kann der Beauftragte dann einschreiten, wenn die Inhaber von Datensammlungen die Grundsätze des Datenschutzes nicht einhalten. Dies bedeutet aber nicht, dass der EDÖB jedes Mal einschreiten kann, wenn eine Person den Eindruck hat, dass ihre Daten missbräuchlich verwendet werden, d. h. ihre Persönlichkeit verletzt wird; nur wenn eine grosse Anzahl von Personen davon betroffen ist, ist der EDÖB zuständig. Bei Einzelfällen obliegt es der betroffenen Person, zivilrechtlich gegen die Persönlichkeitsverletzung vorzugehen.

Privatpersonen sind verpflichtet Datensammlungen beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten anzumelden, wenn diese regelmässig an Dritte bekannt gegeben werden. Diese Verpflichtung gilt auch dann, wenn die betroffenen Personen über den Informationsgebrauch informiert sind.

Die Daten dürfen nur zu dem Zweck genutzt werden, der bei der Beschaffung angegeben wurde. Die Verwendung besonders schützenswerten Personeninformationen ist nur mit Einwilligung der betroffenen Personen gestattet.<sup>15</sup>

Der aktuelle Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragter ist Hanspeter Thür.<sup>16</sup>

---

<sup>15</sup> <http://www.edoeb.admin.ch/datenschutz/00618/00802/00812/index.html?lang=de>

<sup>16</sup> <http://www.edoeb.admin.ch/org/00125/index.html?lang=de>



## 4. Einblick in den politischen Diskurs in der Schweiz

### 4.1 Revision des Datenschutzgesetzes

Das Datenschutzgesetz der Schweiz ist bereits über 20 Jahre alt. In diesen 20 Jahren hat sich mit dem Internet und immer besseren Rechnern eine gewaltige Veränderung vollzogen. Wenn ein Computer in den 90er-Jahren das Einmaleins beherrschte, war das schon beachtlich. Heute – im Zeitalter von Big Data – können Hochleistungsrechner in Echtzeit gigantische Mengen an Daten sammeln und auswerten. So kann z.B. mit den Standortdaten in jedem Smartphone nicht nur die aktuelle Verkehrslage berechnet werden, sondern sogar die zukünftige Lage des Verkehrs.

Berechtigerweise kam deshalb in den letzten Jahren die Frage nach der Aktualität unseres Datenschutzes auf. Im Jahre 2011 hat der Bund deshalb eine Evaluation des DSG durchgeführt und ist zum Schluss gekommen, dass sich das DSG grundsätzlich bewährt, es mit den aktuellen technischen Möglichkeiten jedoch in einigen Fällen den Schutz der Persönlichkeit nicht mehr genügend zu gewährleisten vermag. Der Bundesrat legte folgende Zielsetzung fest, um die Mängel zu beheben:<sup>17</sup>

- **früheres Greifen des Datenschutzes:** Datenschutzprobleme sollen schon bei der Entwicklung neuer Technologien festgestellt und geprüft werden. Daneben sollen datenschutzfreundliche Technologien gefördert werden.
- **verstärkte Sensibilisierung der betroffenen Personen:** Die betroffenen Personen sollen stärker für die mit den technologischen Entwicklungen einhergehenden Risiken für den Persönlichkeitsschutz sensibilisiert werden.
- **Erhöhung der Transparenz:** Die Transparenz über Datenbearbeitungen soll erhöht werden, insbesondere in den neuen komplexen Konstellationen, in denen Datenbearbeitungen weder für die Betroffenen noch für den EDÖB ohne Weiteres erkennbar sind. Dabei wird aber im Auge zu behalten sein, dass die betroffenen Personen nicht mittels einer Informationsflut überfordert werden.
- **Verbesserung der Datenkontrolle und -herrschaft:** Die Kontrolle und die Herrschaft über einmal bekannt gegebene Daten sind ein wichtiger Aspekt. Es soll geprüft werden, ob die Aufsichtsmechanismen des EDÖB gestärkt und ob die Rechtsansprüche der Betroffenen ausgebaut werden sollen.

Besonderes Augenmerk will der Bundesrat dem Schutz von Minderjährigen zuteilen: «Dem Umstand, dass sich Minderjährige der Risiken und Folgen der Verarbeitung personenbezogener Daten weniger bewusst sind als Erwachsene, soll Rechnung getragen werden.»<sup>18</sup>

---

<sup>17</sup> 29.Oktober 2014; Normkonzept zur Revision des Datenschutzgesetzes

<sup>18</sup> <http://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2015/2015-04-010.html>

Im Frühjahr dieses Jahres liess der Bundesrat verlauten, dass bis spätestens Ende August 2016 das Eidgenössische Justiz- und Polizeidepartement einen Vorentwurf für eine Revision des DSG vorlegen soll. Gestützt wurde dieser Entscheid auf einem Expertenbericht des Jahres 2014. Vertreter aus der Verwaltung, der Wissenschaft, der Kantone sowie der Wirtschafts- und Konsumentenverbände diskutierten dabei auf Geheiss des Bundesrates die Notwendigkeit einer Verschärfung/Anpassung des DSG. Es herrschte allerdings keine Einigkeit zwischen den verschiedenen Vertretern. Die Wirtschaftsorganisationen – eine Minderheit in der Gruppe – waren der Ansicht, das geltende Recht genüge, während die restlichen Vertreter eine Revision des Gesetzes für nötig hielten.<sup>19</sup>

So meint der Wirtschaftsdachverband Economiesuisse in einer Stellungnahme, dass das garantierte Schutzniveau im internationalen Vergleich bereits hoch und eine Verschärfung gerade im Privatbereich unnötig sei: «Ein überzogenes, <veradministrirtes> Datenschutzrecht würde die Schweiz global gesehen ins Hintertreffen bringen.» Dem schliesst sich der Schweizerische Gewerbeverband an. In einer neuen Mitteilung lehnt er «zusätzliche Regulierung und Bürokratie im Datenschutz ab». Insbesondere Massnahmen wie generelle Informationspflichten für jegliches Bearbeiten von Daten seien «unverhältnismässig» und erschwerten die gewerbliche Tätigkeit.<sup>20</sup>

Für die Befürworter der Revision ist hingegen klar, dass nun endlich dafür gesorgt werden muss, dass das verfassungsmässige Recht auf Privatsphäre und informelle Selbstbestimmung jedes Einzelnen umgesetzt wird.

Mit der Reform der Datenschutzgesetzgebung steht die Schweiz nicht allein da. Auch die EU revidiert im Moment ihre Datenschutzbestimmungen. Für die Befürworter der Revision ist klar, dass die Schweiz die gegenwärtigen Diskussionen und Entwicklungen beachten muss. Die Schweiz hat einen regen Datenaustausch mit der EU, grosse Unterschiede im Datenschutz könnten für die Zusammenarbeit hinderlich sein.<sup>21</sup>

## 4.2 Zwei umstrittene Gesetzesvorlagen

In der Sommersession 2015 stimmte National- und Ständerat über zwei Gesetzesvorlagen ab, welche den Datenschutz betreffen – die Revision des BÜpf (Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs) und des Nachrichtendienstgesetzes. Die beiden Erlasse sind praktisch unter Dach und Fach, die parlamentarischen Kammern müssen nur noch marginale Differenzen bereinigen.

Das Parlament gibt den Strafverfolgern und dem Geheimdienst somit erheblich mehr Kompetenzen, um auf den Datenverkehr der Bürger zuzugreifen. Gegner fürchten

---

<sup>19</sup> 29.Oktober 2014; Normkonzept zur Revision des Datenschutzgesetzes

<sup>20</sup> NZZ, 1.4.2015

<sup>21</sup> <http://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf>

jetzt die Totalüberwachung. An dieser Stelle sollen die beiden Gesetze, sowie Argumente von Gegnern und Befürwortern, kurz beleuchtet werden.

#### 4.2.1 BÜPF

Wie und wann dürfen Behörden unsere Kommunikation mitlesen? Das regelt das BÜPF – das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs.

Das Ziel der Revision ist es, die Überwachungsmöglichkeiten der Strafverfolgungsbehörden an neue technische Gegebenheiten anzupassen.

Hierzu soll unter anderem die Frist für die sogenannte Vorratsdatenspeicherung der Telekommunikationsanbieter ausgedehnt werden. Heute sind Anbieter von Internet oder Telefonie wie Swisscom, Sunrise, Salt oder Cablecom dazu verpflichtet, gewisse Eckdaten unserer Kommunikation zu speichern und aufzubewahren. Gespeichert wird, wer mit wem telefoniert oder E-Mails schreibt, nicht der Inhalt selbst. Auch die ungefähre Position von uns allen wird erfasst.

Die Strafverfolgungsbehörden können in einem laufenden Verfahren auf diese Daten zugreifen. Die Aufbewahrungszeit dieser gesammelten Personendaten soll nun von einem halben auf ein ganzes Jahr verdoppelt werden.

Die Befürworter argumentieren, dass die Verfahren, bis Behörden auf die Daten zugreifen können, lange dauern und somit eine Fristverlängerung nötig sei. Wichtige Daten würden nach einem halben Jahr gelöscht und können so bei späteren Ermittlungen nicht mehr genutzt werden. Dem hält der eidgenössische Datenschutzbeauftragte Hanspeter Thür in einem Interview mit der NZZ entgegen, ihm sei kein Fall bekannt, bei dem die heutige Frist die Aufklärung einer Straftat verhindert habe.<sup>22</sup>

Auf der Gegenseite ist neben der grundsätzlichen Ablehnung dieser Datenspeicherung, welche den Datenschutz verletze, auch der Kostenpunkt ein Thema. Diese zusätzlichen Kosten im zweistelligen Millionenbereich haben die Anbieterfirmen zu tragen und würden auf die Kunden abgewälzt.

Im Weiteren will die Revision den Einsatz sogenannter «Staatstrojaner» ermöglichen. Damit ist eine Software gemeint, die heimlich auf dem Computer eines Verdächtigen installiert wird und dort dann E-Mails oder Internet-Telefonie mitschneiden kann. So könnten auch verschlüsselte Telefonate abgehört werden.

Die Gegner kritisieren die vielen offenen Fragen bei der konkreten Umsetzung. So ist beispielsweise unklar, wie sichergestellt werden soll, dass diese Staatstrojaner den Computer nicht beschädigen, keine Daten darauf verändern und nichts anderes tun können als Kommunikation mitszuschneiden. Ausserdem ist offen, wer diese Software programmiert und wer überprüft, ob sie nur das tut, was sie soll. Auch seien für solche Trojaner Sicherheitslücken im Computersystem nötig. Lücken, welche der Staat eigentlich verhindern und bekämpfen sollte.

---

<sup>22</sup> <http://www.nzz.ch/schweiz/privatsphaere-wird-zu-einem-privileg-1.18256915>

Die Befürworter der Revision betonen, dass die Anpassungen an neue technische Realitäten nötig seien. Wenn Strafverfolgungsbehörden überwachen müssen, brauchen sie auch die nötigen Mittel und Rechte dafür. Die Trojaner würden nur sehr gezielt und mit grösster Vorsicht eingesetzt.<sup>23</sup>

#### 4.2.2 Nachrichtendienstgesetz

Mit dem neuen Gesetz soll der Nachrichtendienst erstmals eine gesamtheitliche Gesetzesgrundlage erhalten und diverse Kompetenzen zur Beschaffung von Personendaten erhalten. So dürfte der Nachrichtendienst künftig Telefonate abhören, Räume verwanzen, Computer hacken und Datenströme im Internet scannen. Künftig soll somit nicht nur Funk- sondern auch Kabelaufklärung möglich sein.

Die Befürworter argumentierten mit der Gefahr terroristischer Anschläge, die zugenommen habe. Ohne Sicherheit gebe es keine Freiheit, lautete der Tenor. Die Schweiz dürfe nicht zu einem Mekka für Terroristen werden – die Kabelaufklärung sei für einen glaubwürdigen Nachrichtendienst zwingend, da ein Grossteil der heutigen Kommunikation über Kabel läuft. «Wenn wir hier nicht tätig werden, ermöglichen wir den Terroristen und Kriminellen, ihr Unwesen zu treiben», sagte Nationalrätin Nadja Pieren. Auch die Ratskollegin Christa Markwalder unterstützt die Vorlage: «Der Nachrichtendienst braucht die nötigen Mittel, um der technologischen Entwicklung folgen zu können. Die Rechtsstaatlichkeit muss gewährt bleiben. Das ist bei dieser Vorlage der Fall.»

Das neue Nachrichtendienstgesetz soll die Sicherheit in der Schweiz erhöhen. Laut dem Tagesanzeiger befürchten RechtsexpertInnen jedoch eine gegenteilige Wirkung. In der Schweiz könnte geschehen, was anderswo schon oft geschah: Ein Terrorist steht zwar unter Beobachtung, wird aber nicht an der Tat gehindert, da die Strafverfolgungsbehörde nicht involviert sei. Mit der heutigen Gesetzeslage sei eine Überwachung von Terroristen möglich, jedoch nur in der Zusammenarbeit mit den Strafverfolgungsbehörden. Dies habe besonders im Ernstfall Vorteile<sup>24</sup>.

Organisationen wie die Digitale Gesellschaft, Amnesty International und die Stiftung für Konsumentenschutz appellierten vergeblich an die PolitikerInnen, die Kabelüberüberwachung aus dem Gesetz zu streichen. Diese Überwachung sei die „Suche nach der Nadel im Heuhaufen“ – ein Tritt gegen die Verhältnismässigkeit, bei dem viele unbescholtene BürgerInnen ausspioniert würden. Dieses Gesetz ebne den Weg zu einem Überwachungsstaat – denn ob sich der Schweizer Geheimdienst im Gegensatz zu ausländischen Diensten immer an die gesetzlichen Grenzen halten werde, sei fraglich und kaum zu kontrollieren. Die Revision sei deshalb eines freien und demokratischen Landes unwürdig. Unterstützt wurden diese Bedenken im

---

<sup>23</sup><http://www.srf.ch/wissen/digital/das-will-das-neue-buepf-daten-laenger-speichern-und-staatstrojaner>

<sup>24</sup> <http://www.tagesanzeiger.ch/schweiz/Neues-Nachrichtendienstgesetz-koennte-Terroristen-beguenstigen/story/26225799>

Parlament lediglich von den Grünen und Teilen der SP – in Zeiten wo der IS und andere radikale Organisationen Angst und Schrecken verbreiten, keine verwunderliche Entwicklung. Auch wenn die Anschläge in Frankreich aus Sicht der Gegner des neuen Gesetzes zeigen, dass selbst ein Top-Geheimdienst - wie der der Grande Nation - dem Terror oft das Handwerk nicht rechtzeitig legen kann.<sup>25</sup>

Gegner beider Gesetzesrevisionen haben Referenden angekündigt. Hier bilden sich ungewöhnliche Allianzen, besonders unter den Jungen. So unterstützt ein Grossteil der Jungparteien – von Jusos bis JSVP - die Petition „Stopp Büp“.<sup>26</sup>

## 5. Datenschutz – eine globale Herausforderung

Edward Snowden hat mit seinen Enthüllungen über die weltweiten Überwachungs- und Spionagepraktiken der NSA (National Security Agency; Auslandsgeheimdienst der USA) für einen weltweiten Aufschrei gesorgt. Was eigentlich schon lange klar war, wurde nun in den Medien ein grosses Thema. Seither scheint sich ein Abhörskandal nach dem anderen zu ereignen. Laut den Enthüllungen wird vor allem Deutschland von der NSA in gigantischen Ausmassen bespitzelt. Der Spiegel schrieb: Wir alle sind Opfer des größten Spionageskandals aller Zeiten! Das anfängliche Schweigen der Bundeskanzlerin zum Abhörskandal, brach erst als bekannt wurde, dass selbst Frau Merkel ausspioniert wurde.

Bis auf Großbritannien, Kanada, Australien und Neuseeland, die mit den USA die sogenannten „Five Eyes“ bilden, muss die Spionagebehörde der USA vor keiner Regierung haltmachen.<sup>27</sup> So sind auch sämtliche Präsidenten Frankreichs der letzten Jahre unter den Opfern.

Bis heute veröffentlichten die Medien einen Skandal nach dem anderen und längst ist klar, dass nicht nur der Geheimdienst der USA betroffen ist. Spioniert wird weltweit, die Geheimdienste arbeiten zusammen und gehen mit den Personendaten der Bevölkerung aus Sicht vieler DatenschützerInnen äusserst fragwürdig um. Auch der deutsche Bundesnachrichtendienst sei kein unschuldiges Lamm. So veröffentlichte die NZZ Dokumente, die belegen sollen, dass die NSA in Zusammenarbeit mit dem BND Swisscom Kunden ausspionierte.<sup>28</sup>

Diese Affären zeigen vielen Politikern in Europa, dass ein nationaler Datenschutz oft wirkungslos ist. In einer vernetzten und globalisierten Welt braucht es Datenschutzrichtlinien, welche weltweit anerkannt sind, damit dem Missbrauch von Personenda-

---

<sup>25</sup> <http://www.srf.ch/news/schweiz/session/pro-und-contra-mehr-kompetenzen-fuer-den-nachrichtendienst>

<sup>26</sup> <http://buepf.ch/>

<sup>27</sup> <http://www.taz.de/!5038752/>

<sup>28</sup> <http://www.nzz.ch/schweiz/bnd-und-nsa-sollen-swisscom-kunden-ausspioniert-haben-1.18549890>

ten ein Ende gesetzt werden kann. Datenschutz muss in einer globalen Dimension betrachtet werden.

Heute betreiben viele Geheimdienste einen regen Tauschhandel. Daten welche ein Geheimdienst auf Grund der Gesetzeslage im eigenen Land nicht erheben darf, werden einfach mittels eines ausländischen Dienstes ermittelt. Dieser erhält dann im Gegenzug Daten, zu welchen er keinen Zugang hat. So steht zum Beispiel die NSA in einem intensiven Austausch mit dem britischen Geheimdienst und kann so US-Recht umgehen. Schweizer Geheimdienstexperten sind überzeugt, dass viele westliche Länder an diesem Tauschhandel beteiligt sind – auch die Schweiz. Nicht zuletzt will das neue Nachrichtendienstgesetz wohl die Position der Schweiz in diesem Datenhandel stärken. So heisst es im Artikel 10 des neuen Gesetzes explizit, der NDB (Nachrichtendienst des Bundes) dürfe zur Erfüllung seiner Aufgabe «mit ausländischen Nachrichtendiensten und Sicherheitsbehörden zusammenarbeiten».<sup>29</sup>

«Ich gehe davon aus, dass der NDB, wie jeder europäische Geheimdienst, Verbindungen zur NSA unterhält», sagte Geheimdienstexperte Erich Schmidt-Eenboom. Der NDB sei auf Informationen der NSA angewiesen, und umgekehrt werde der NDB auch Daten liefern. «Geheimdienstarbeit ist ein Geben und Nehmen»<sup>30</sup>

In wie weit all diese Spionageaktivitäten immer nur der Sicherheit der Bevölkerung dienen, sollte offen hinterfragt werden. Nationale Interessen – ob wirtschaftlich oder machtpolitisch – scheinen eine ebenso wichtige Rolle zu spielen. Vor allem die USA steht in diesem Zusammenhang unter weltweiter Kritik<sup>31</sup>

Will man den globalen Datenschutz stärken, so ist die Mitarbeit der USA zwingend. Nicht nur die NSA, sondern auch viele globale Internetriesen wie Google, Facebook, Amazon und Co. Sammeln weltweit gigantische Mengen an Personendaten. Doch der Datenschutz hat in den Vereinigten Staat von Amerika einen schweren Stand – vor allem die wirtschaftlichen Interessen scheinen dem Schutz der Privatsphäre im Wege zustehen.<sup>32</sup>

## 6. Datenschutz und Eigenverantwortung

Die meisten Leute sind sich nicht bewusst, wo überall ihre persönlichen Daten gesammelt werden. Ob beim Punktesammeln im Supermarkt, beim Ausfüllen eines Wettbewerbes, oder bei jeglicher Aktivität im Internet – Datensammler sind omnipräsent. Es ist heute für den Staat sehr schwierig unsere Privatsphäre vor

---

<sup>29</sup> <http://www.nzz.ch/schweiz/geheimdienst-soll-daten-einfacher-ins-ausland-liefern-koennen-1.18177437>

<sup>30</sup> <http://www.nzz.ch/schweiz/geheimdienst-soll-daten-einfacher-ins-ausland-liefern-koennen-1.18177437>

<sup>31</sup> <http://www.handelsblatt.com/politik/deutschland/wikileaks-und-taeglich-gruesst-die-nsa/12034888.html>

<sup>32</sup> <http://www.spiegel.de/netzwelt/netzpolitik/datenschutz-in-den-usa-und-europa-a-849114.html>

Missbrauch zu schützen. Eine grosse Wichtigkeit im Datenschutz kommt deshalb der Eigenverantwortung zu.

Vor allem vor Missbrauch im Internet, ist die eigene Sorgfalt entscheidend. Was einmal im Internet ist, kann meist nicht mehr gelöscht werden, auch vom besten Staat nicht. Rechtlich sind wir ja eigentlich vor Missbrauch unserer Daten im Internet „geschützt“, denn Dritte dürfen unsere Daten nicht veröffentlichen ohne unsere Erlaubnis. Nur bietet allein „das Recht und Gesetz“ keinen ausreichenden Schutz. Denn der angerichtete Schaden, z.B. durch die Verbreitung intimer Fotos, kann kein Gerichtsurteil wieder rückgängig machen.

Im Datenschutz spielt deshalb die **Eigenverantwortung** eine zentrale Rolle. Ein verantwortungsvoller Umgang mit den eigenen Daten kann schon sehr viel bewirken. In der heutigen Welt ist es unmöglich, keine persönlichen Daten preiszugeben. Entscheidend scheint zu sein, dass sich die Menschen so gut es geht bewusst sind wo, welche Daten von ihnen gesammelt werden und dass sie sich im Klaren sind, welche persönlichen Daten sie mit der Öffentlichkeit teilen wollen und welche nicht. Der EDÖB schenkt deshalb der Sensibilisierung der Bevölkerung grosses Gewicht. Eine Sensibilisierung, die noch grosse Potenzial in sich trägt.<sup>33</sup>

Laut dem obersten Datenschützer der Schweiz, Hanspeter Thür, seien sich viele Nutzer der Datensammlung im Netz bewusst, doch möchten die wenigsten deshalb auf die Dienste von Facebook oder Google verzichten: «Man will einen Service, einen Dienst, ein Produkt – aber man bekommt es nur, wenn man das Feld «Ich akzeptiere» anklickt.» Dieses unfaire Gefälle zwischen Anbieter und Konsument sollte laut Thür abgebaut werden, hier sei die internationale Politik gefragt.<sup>34</sup>

In der ganzen Diskussion um den Datenschutz ist es am Staat Rahmenbedingungen festzulegen, die Eigenverantwortung im Umgang mit deinen Daten wird er dir jedoch nicht abnehmen können.

Zum Schluss zwei Zitate von zwei einflussreichen Deutschen, die dich vielleicht zum Nachdenken anregen können.

Wolfgang Schäuble (Politiker CDU) nimmt in der Zeitung Die Welt Stellung zum NSA-Sakndal: „*Wenn Sie in der Öffentlichkeit sind, müssen Sie damit rechnen, dass Sie beobachtet werden.*“<sup>35</sup>

Der vor zwei Jahren verstorbene Kabarettist und Autor Dieter Hildebrandt hätte dem wohl nur eines anzufügen: „*Mich regt die Tatsache auf, dass sich niemand aufregt.*“<sup>36</sup>

---

<sup>33</sup> <http://www.edoeb.admin.ch/datenschutz/00618/00802/00814/index.html?lang=de>

<sup>34</sup> <http://www.tagesanzeiger.ch/schweiz/standard/Ich-wuerde-nie-ueber-einen-USService-mailen/story/23317779?track>

<sup>35</sup> Interview mit *welt.de* am 4. Februar 2007, [bmi.bund.de](http://www.bmi.bund.de)

<sup>36</sup> Interview mit Süddeutsche Zeitung 23. Mai 2012, 09:11 Uhr

## 7. Weitere Informationen

Du möchtest mehr über den Datenschutz erfahren?

Folgende Links helfen dir weiter:

Datenschutz Schweiz

<http://www.edoeb.admin.ch/>

<https://www.admin.ch/opc/de/classified-compilation/19920153/>

<http://www.it-recht.ch/wp-content/uploads/2014/11/Folien-Straub-Einfuehrung-ins-Datenschutzrecht-Uni-FR-06.12.2004.pdf>

<https://dsb.zh.ch/internet/datenschutzbeauftragter/de/home.html>

<http://www.ictlaw.ch/datenschutz-schweiz-139.htm>

<http://www.datenschutz-forum.ch/>

Datenschutz Europa

<http://www.bpb.de/gesellschaft/medien/datenschutz/>

<https://www.datenschutzzentrum.de/material/recht/eu-datenschutzrichtlinie.htm>

[http://www.bmi.bund.de/DE/Themen/Gesellschaft-Verfassung/Datenschutz/Datenschutzrecht-EU/datenschutzrecht-eu\\_node.html](http://www.bmi.bund.de/DE/Themen/Gesellschaft-Verfassung/Datenschutz/Datenschutzrecht-EU/datenschutzrecht-eu_node.html)

Hilfreiche Videos :

Einstein Sendung zu Big Data: <http://www.srf.ch/sendungen/einstein/einstein-spezial/einstein-spezial-big-data>

Datenschutz einfach erklärt: <https://www.youtube.com/watch?v=VF5A2JhiJug>

Und hier kannst du die Dimensionen des weltweiten Internet-Datenverkehrs verfolgen - *The Internet in Real-Time*: <http://pennystocks.la/internet-in-real-time/>