

2016



Grünbuch Digital Society

Problemsammlung Digital Society – März 2016

ENTWURF

Version 0.8 – 20.03.2016

Redaktion: Werner Illsinger

Herzlichen Dank an alle Mitwirkenden. Im Besonderen an:

Roland Giersig, Andrea Illsinger, Georg Tsamis; Erich Pekar

für Beiträge und Mitarbeit am vorliegenden Grünbuch.



Digital Society CC BY-NC-SA 3.0 AT

Zusammenfassung: Teilen, verändern, darauf aufbauen ist erlaubt unter der Voraussetzung der Namensnennung, nicht kommerziellen Verwendung, sowie Weitergabe unter gleichen Bedingungen.

Contents

1	Allgemeines	7
1.1	Was ist ein Grünbuch	7
1.2	Ziel des Grünbuches	7
1.3	Aufbau.....	7
2	Digital Society.....	9
2.1	Vision der Digital Society.....	9
2.2	Mission der Digital Society	9
2.3	Einladung zur Teilnahme	9
3	Digitalisierung.....	10
4	Veränderung der Gesellschaft durch die Digitalisierung	12
4.1	Arbeitswelt	12
4.1.1	Veränderungen in der Arbeitswelt	12
4.1.2	Stakeholder in der digitalen Arbeitswelt	12
4.1.3	Faktor Zeit.....	13
4.1.4	Faktor Ort.....	14
4.1.5	Schutz der Arbeitnehmer	14
4.1.6	Anforderungen an die Arbeitnehmer	15
4.1.7	War of Talents.....	16
4.1.8	Führen in der digitalen Welt.....	16
4.1.9	Veränderung von Jobs	17
4.2	Wirtschaft.....	18
4.2.1	Steuergesetzgebung	18
4.2.2	Cloud-Computing	22
4.2.3	Produktion und Industrie 4.0	25
4.2.4	3D Printing.....	25
4.2.5	Internet of Things (IoT)	26

4.2.6	Big Data & Datenhandel	27
4.2.7	Online Vertriebswege	28
4.2.8	Digitale Werbung und Marketing	29
4.2.9	Zahlungsverkehr	29
4.3	Privatleben & Familie	31
4.3.1	Digital Divide / Digitale Kluft	31
4.3.2	Smartphones & Devices	32
4.3.3	Wearables	33
4.3.4	Fotografie und Video	33
4.3.5	Medienkonsum	34
4.3.6	Einkaufen	35
4.3.7	Bankgeschäfte	36
4.3.8	Automobil	37
4.4	Bildung & Forschung	39
4.4.1	Forschung und Innovation	39
4.4.2	Bildung	43
5	Grundrechte	49
5.1	Welche Grundrechte gibt es?	49
5.2	Meinungsfreiheit	50
5.3	Brief- Kommunikationsgeheimnis	51
5.3.1	Vorratsdatenspeicherung	52
5.4	Fluggastdaten / Passenger Name Record (PNR)	53
5.4.1	Was sind Fluggastdaten / Passenger Name Record (PNR)	53
5.4.2	Fluggastdatenaustausch EU / USA	54
5.4.3	Innereuropäische Fluggastdatenspeicherung	55
5.5	Staatsschutzgesetz	57
6	Urheberrecht & digitale Medien	58

6.1	Faire Entlohnung für künstlerische Arbeit.....	58
6.2	Privatkopie und Publikum	59
6.3	Überwachung.....	59
6.3.1	Nachteile für ehrliche Käufer.....	60
6.4	Veränderungen in der Medienlandschaft	61
6.5	Festplattenabgabe / Speichermedienabgabe	62
7	Datenschutz.....	64
7.1	Recht auf informationelle Selbstbestimmung.....	64
7.2	Schutz Personenbezogener Daten	64
7.3	Anwendung des Datenschutzes	65
7.4	Safe Harbour	66
7.5	Passenger Name Record (PNR)	66
7.6	ELGA.....	66
7.7	E-Call	69
7.8	Smartmeter	70
8	Transparente öffentliche Verwaltung.....	71
8.1	Verwaltungstransparenz	71
8.2	Digitale Demokratie / E-Democracy.....	72
8.3	E-Government.....	73
8.4	Open Data	74
9	Infrastruktur.....	76
9.1	Frei verfügbares und neutrales Internet	76
9.2	Zugängliches Internet	77
9.3	Sicherheit der Infrastruktur.....	77
9.4	Breitbandausbau	79
9.5	Netzneutralität.....	81
9.5.1	Beispiele für Verletzungen von Netzneutralität.....	83

10	Andere Institutionen.....	85
10.1	Private Vereine / Zivilgesellschaft.....	85
10.1.1	Verein der Internet Benutzer VIBE.....	85
10.1.2	AK Vorrat.....	85
10.1.3	Open3.....	85
10.1.4	Österreichische Computer Gesellschaft.....	85
10.1.5	Forum für Informationsfreiheit (FOI).....	86
10.1.6	Forum Datenschutz.....	86
10.1.7	Neuwal.com.....	87
10.1.8	Qualitätszeit.at.....	87
10.1.9	Digitalista.at.....	87
10.1.10	Open Knowledge Austria.....	88
10.2	Regierungsnahe Organisationen / Vereine.....	88
10.2.1	Werdedigital.at.....	88
10.2.2	Saferinternet.at.....	88
10.3	Wirtschaftsnahe Organisationen & Vereine.....	89
10.3.1	ISPA Internet Service Providers Austria (ISPA).....	89
10.3.2	Verein für Anti Piraterie der Film und Videobranche (VAP).....	89
10.3.3	Verband Alternativer Telekom Netzbetreiber.....	90
10.3.4	Verband Österreichischer Zeitungen (VÖZ).....	90
10.4	Europäische Organisationen.....	90
10.4.1	European Digital Rights.....	90
11	Staatliche Stellen (EU / Österreich / Länder / Gemeinden).....	94

1 Allgemeines

1.1 Was ist ein Grünbuch

Ein **Grünbuch** ist ein Instrument das vor allem aus der Europäischen Kommission bekannt ist. Ein Grünbuch ist ein Diskussionspapier zu einem bestimmten Thema, mit dem Zweck, auf diesem Gebiet eine öffentliche und wissenschaftliche Diskussion herbeizuführen und grundlegende politische Prozesse in Gang zu setzen.

Häufig wird eine Reihe von Ideen oder Fragen aufgeworfen und Einzelne sowie Organisationen werden zu Beiträgen aufgefordert. Nächster Schritt ist oft ein Weißbuch, welches offizielle Lösungsvorschläge zusammenfasst.

Ziel dieses Grünbuches ist es Problembereiche und Fragen zur Digitalisierung unseres Lebens aufzuwerfen und zur Diskussion anzuregen. Wir wollen in diesem Grünbuch keine fertigen Lösungen oder Patentrezepte präsentieren. Wir laden aber andere Personen und Institutionen herzlich ein sich in den Prozess einzubringen und ihre Ideen und Lösungsvorschläge einzubringen.

1.2 Ziel des Grünbuches

Ziel des Grünbuchs ist es, im ersten Schritt Problembereiche durch die Digitalisierung unserer Gesellschaft aufzuzeigen. Im zweiten Schritt sollen Lösungsmöglichkeiten erarbeitet und Pro und Kontra der verschiedenen Möglichkeiten aufgezeigt werden.

Bei der Erarbeitung soll darauf geachtet werden, dass die Digital Society nicht als „Maschinenstürmer“ oder „Blockierer“ gesehen wird. Technologischer Fortschritt ist wichtig, und wir befürworten ihn, aber der Fortschritt kann nicht zu Lasten der Grundrechte und der Bürger gehen, und allgemein etablierte Gesetze der „analogen Welt“ müssen auch in der digitalen eingehalten werden.

1.3 Aufbau

Das Buch ist in Kapitel gegliedert. In jedem Kapitel werden die Problembereiche textuell beschrieben. Kästen in Rot fassen die Problembereiche zusammen:



- Zusammenfassung.

Kästen in grauer Farbe stellen Forderungen oder Lösungsvorschläge dar. Dabei wird dokumentiert, von wem diese Lösungsvorschläge eingebracht wurden, oder wer diese Position unterstützt:

	Forderung der Digital Society: • Forderung / Lösungsvorschlag und an wen diese gerichtet ist.
---	--

2 Digital Society

2.1 Vision der Digital Society

Unsere Vision ist eine **freie digitale Welt**, in der die **öffentliche Verwaltung transparent** und die **Privatsphäre geschützt**, das **Internet offen**, neutral und der Zugang zu Wissen und dem Netz frei ist. **Firmen und Konsumenten agieren als Partner** zu ihrem gemeinsamen Vorteil.

2.2 Mission der Digital Society

Die Digital Society möchte über technologische, gesellschaftliche und rechtliche Aspekte **informieren**. Damit soll erreicht werden, dass Bürger sowie Politiker sich **auf Fakten basierende Meinungen** bilden können. Aus diesen sollen Gesetze entstehen, die dem **gemeinsamen Nutzen von Konsumenten und Wirtschaft** in der digitalen Welt dienen. Die **Grundrechte** der analogen Welt müssen auch in der digitalen Welt etabliert und verteidigt werden.

2.3 Einladung zur Teilnahme

Wir möchten als Digital Society alle Stakeholder einladen mitzumachen. Wir glauben gemäß unserer Vision, dass ein gedeihliches Zusammenleben nur unter Einbindung aller Stakeholder und durch faktenbasierte Entscheidungsprozesse möglich ist.

Wir möchten auch um den Vorgang transparent zu machen dort wo Dissens herrscht diesen vorerst nicht auflösen, sondern dokumentieren und auch die Quellen angeben.

3 Digitalisierung

Die Digitalisierung verändert derzeit grundlegend unsere Gesellschaft. Der Prozess ist schon seit längerer Zeit im Gange. Beispielsweise wurde in der Fotografie der Film fast vollständig durch digitale Medien abgelöst. Briefe werden nur noch zu besonderen Anlässen von Hand geschrieben und die Anzahl von Briefen ist vernachlässigbar gegenüber den versendeten E-Mails pro Tag.

Die Digitalisierung unserer Welt wird aber nicht langsamer – im Gegenteil, die Geschwindigkeit nimmt rasant zu. Man könnte die Veränderungen in unserer Welt durchaus mit der industriellen Revolution vergleichen. Es gibt viele positive Entwicklungen und viele neue Chancen durch diese Entwicklung. Aber auch Ängste wie zum Beispiel vor Jobverlust. Für Unternehmen gilt hier ebenfalls – entweder die Unternehmen stellen sich auf die Veränderungen ein, oder es könnte sie schon morgen nicht mehr geben. Uber macht Taxiunternehmen Konkurrenz – und Airbnb mit Couch Surfing etablierten Hotels Konkurrenz – und der Einzelhandel steht unter Druck seitens Amazon, Alibaba¹Rakuten².

Die neuen Möglichkeiten beinhalten auch Gefahren. Das gesamte Leben von Menschen ist mittlerweile digital. Das birgt auch die Gefahr vor Missbrauch dieser Daten. Spätestens seit Edward Snowden wissen wir, dass sich Regierungen bei der Überwachung ihrer eigenen Bevölkerung auch nicht an Gesetze halten. Die Terrorgefahr dient allzu oft als Vorwand, um die Bevölkerung davon zu überzeugen, dass diese ungerechtfertigte Massenüberwachung nur zu ihrem Besten ist. Aber auch seit Max Schrems wissen wir, dass Facebook (und sicher auch viele andere Konzerne) geltendes Datenschutzrecht nicht einhalten und Regierungen und zuständige Behörden sich oft überfordert fühlen.

¹ Alibaba bzw. Aliexpress ist die größte internationale Handelsplattform, die hauptsächlich fernöstliche Produzenten mit westlichen Händlern und Konsumenten zusammen bringt.

² RAKUTEN ist eines der 10 größten Internet Unternehmen, das vor allem durch Akquisitionen entstanden ist.

Dieser Umgang mit dem Internet birgt aber auch die Gefahr, dass ein neues Biedermeier entsteht: Menschen verlieren das Vertrauen in das Medium und verwenden es nur noch anonym unter falschem Namen. Firmen haben berechtigte Ängste, dass ihre Betriebsgeheimnisse ausspioniert werden – und verwenden neue Technologien (wie Cloud-Computing) nicht. Menschen und Unternehmen müssen dabei unterstützt werden, dass sie ihre Daten auch vor ungerechtfertigtem Zugriff schützen.

Die Digitalisierung birgt aber auch gesellschaftliche Herausforderungen. Beispielsweise macht eine elektronische Zustellung von Schriftstücken und Rechnungen durchaus Sinn, aber dazu müssten alle Empfänger (Bevölkerungsgruppen) auch in der Lage sein, diese zu empfangen. Die „digitale Kluft“ muss geschlossen werden. Heute gibt es Förderungen für Telefonanschlüsse und Fernsehen – aber sollte es diese nicht für das Internet geben?

4 Veränderung der Gesellschaft durch die Digitalisierung

4.1 Arbeitswelt

4.1.1 Veränderungen in der Arbeitswelt



Technologie verändert unsere Arbeitswelt grundlegend. Die Gewerkschaften fordern mehr Urlaub und pochen auf die Einhaltung der Wochenendruhe und 38,5 Stunden Woche. Haben diese Begriffe aber noch Relevanz, wenn man dank Mobiltelefon und Internet eigentlich ständig arbeitet oder arbeiten könnte? "My Office is where I am" – verkünden Technologiekonzerne stolz. Ich sitze zu

Hause auf der Terrasse, schaue in den Garten und arbeite dabei. Das kann durchaus zum Nutzen des Arbeitnehmers, aber auch zum Nutzen des Arbeitsgebers sein - auf die Randbedingungen kommt es an. Wie müssen Regelungen aussehen, die mit der faktischen Situation im Jahre 2015 zusammenpassen und die Arbeitnehmer trotzdem vor Ausbeutung schützen?

4.1.2 Stakeholder in der digitalen Arbeitswelt

Die Stakeholder sind vor allem die **Arbeitnehmervertreter** wie Arbeiterkammer und ÖGB, sowie die **Vertreter der Wirtschaft** wie Wirtschaftskammer, Industriellenvereinigung und andere Berufs- und Standesvertretungen, aber auch **Technologieunternehmen** die die entsprechenden Szenarien erst möglich machen. In manchen Industrien aber auch Regulatoren. Einige der Regularien nehmen auf aktuelle Entwicklungen keine Rücksicht und müssen überprüft und angepasst werden.

Viele der oben genannten Stakeholder müssen sich auf die veränderte Situation durch die Möglichkeiten der Digitalisierung auch erst einstellen und benötigen teilweise auch Hilfestellungen und Aufklärung in diesem Bereich.

4.1.3 Faktor Zeit

Die Stechuhr ist sicherlich noch immer in vielen produzierenden Unternehmen vorhanden und nicht wegdenkbar. In anderen Branchen ist sie aber ein Relikt aus einer vergangenen Epoche, veraltet und vielfach hinderlich. **Die im Büro verbrachte Arbeitszeit ist heute kein Messkriterium für Arbeit mehr.**

Internet und Mobiltelefon und moderne Technologien wie Cloud-Computing und Telekonferenzen ermöglichen, dass wir immer und überall arbeiten können – und die Erwartungshaltung der Unternehmen ist zunehmend auch, dass die Arbeitnehmer immer und überall erreichbar sind. In der Nacht, am Wochenende – und im Urlaub. **Die Grenzen zwischen Privatleben und Arbeit sind daher oft sehr verschwommen.** Der Mitarbeiter muss darauf achten, dass er nicht zu einem Workaholic wird – und seine Balance zwischen Privat und Familienleben erhält.

Für den **Arbeitnehmer** können flexible Arbeitszeiten in Unternehmen sicherlich hilfreich sein, denn er kann sich seine Zeit freier und besser einteilen, kann auf seine familiäre Situation Rücksicht nehmen, aber auch z.B. auf Verkehrssituationen. Er kann später in die Arbeit fahren um dem morgendlichen Stau zu entgehen.

Für den **Arbeitgeber** ist diese Flexibilisierung hilfreich. Er kann Mitarbeiter besser einsetzen, aber auch für den Arbeitgeber ergibt sich das Problem, dass die Messung der erbrachten Arbeit nicht mehr aufgrund von Anwesenheit erfolgen kann. Die Messung muss anders erfolgen – meist über Leistung. Und der Arbeitgeber muss seinen Mitarbeitern ein weitaus höheres Vertrauen entgegenbringen.



- Größere Flexibilisierung der Arbeitszeiten.
- Größeres Vertrauen in die eigenen Mitarbeiter durch die Unternehmen notwendig.
- Mitarbeiter müssen ein ausgezeichnetes Betriebsklima vorfinden und gut motiviert sein.
- Neuregelung für die Messung von Arbeit & Bezahlung notwendig
- Überprüfung von arbeitsrechtlichen Bestimmungen für die Anwendbarkeit in der heutigen Zeit notwendig

4.14 Faktor Ort

Information Worker können immer und überall arbeiten. Sobald Geschäftsprozesse digitalisiert sind, und die Informationen elektronisch zur Verfügung stehen kann die Arbeit im Büro, im Kaffeehaus und auch am Badeteich erbracht werden. Das Internet und die ständige Vernetzung, sowie die mobilen Geräte (Notebook, Tablett, Smartphone machen diese Entwicklung möglich). "My Office is where I am", das ist das Schlagwort. Man geht nicht mehr in die Arbeit. Man ist überall in der Arbeit.



- Unternehmen müssen die vorhandenen Technologien auch nutzen und ihren Mitarbeitern anbieten
- Prozesse müssen digitalisiert werden. Nur wenn keine physischen Unterlagen erforderlich sind, ist auch Arbeit überall möglich.
- Dafür ist eine Sensibilisierung und Aufklärung auch für die Unternehmen notwendig.
- In diesem Zusammenhang sind auch die Themen Cloud-Computing und Bring your Own Device Strategien (BYOD) zu betrachten.
- Aufgrund der veränderten Anforderungen müssen sich auch die Büros verändern und den neuen Anforderungen anpassen.

4.15 Schutz der Arbeitnehmer

Arbeitnehmerschutzregelungen existieren, sie sind jedoch teilweise unflexibel und nicht immer anwendbar, aus praktischen wie wirtschaftlichen Gründen. Nach den derzeitigen Regelungen müssten vermutlich ein Gutteil aller "Information Worker" in Dauerbereitschaft bezahlt werden, weil sie im Grunde rund um die Uhr erreichbar sind. Früher bedeutete Bereitschaft eine massive Einschränkung der Bewegungsfreiheit, musste man doch in Hörweite eines Festnetztelefons und des Computers sein. Handy, Notebook und mobile Datenübertragung haben hier die Bewegungsfreiheit massiv ausgeweitet, sodass in Normalsituationen nur mehr eine geringe Einschränkung besteht. Aktuelle Regelungen nehmen auf diese geänderten Umstände nicht immer Rücksicht.

Die Forderungen der Gewerkschaften nach Reduktion der Arbeitszeit klingen daher antiquiert, fast wie aus dem vorigen Jahrhundert. Wie soll man etwas reduzieren, das nicht einmal mehr wirklich messbar ist. Wie könnten aber Regelungen aussehen, die zum Nutzen der Arbeitnehmer und zum Wohle der Arbeitgeber sind?

Teilweise fördern diese Arbeitnehmerschutzregelungen sogar, dass Mitarbeiter nicht mehr fest angestellt werden, um diesen Regelungen zu entgehen. So sind Paketboten meist (schein-)selbständige Unternehmer. Damit gelten Kollektivverträge und Arbeitszeitregelungen nicht mehr. Diese Entwicklung ist aber auch in anderen Bereichen erkennbar. Auf der anderen Seite gibt es derzeit eine heftige Diskussion um Freiberufler in der IT – die zwangsangestellt werden sollen – obwohl gerade diese Unternehmer die Freiheit der Selbständigkeit genießen, und diese gar nicht aufgeben wollen. Natürlich ist eine Diskussion erforderlich wie Zustände verhindert werden, wie sie im Transportwesen (Paketboten) lange schon Realität sind.

4.1.6 Anforderungen an die Arbeitnehmer

Auch muss der Arbeitnehmer von heute anders arbeiten als früher. Man verlangt von ihm, dass er sehr **flexibel und eigenverantwortlich** arbeitet, **teamfähig** ist und wie ein Unternehmer denkt. Oftmalig wird daher auch eine feste Anstellung durch ein freies Dienstverhältnis ersetzt. Die Mitarbeiter arbeiten auf Projektbasis. **Die Sicherheit der festen Anstellung gibt es nicht mehr.** Sie ist sogar im staatlichen Umfeld nur noch selten. Beamte wurden Großteils durch Vertragsbedienstete ersetzt.



- Arbeitnehmer müssen auf diese Entwicklungen besser vorbereitet werden. Hier muß schon im Schulsystem angesetzt werden, aber auch „lebenslanges Lernen“ tatsächlich gelebt werden.
- Mitarbeiter müssen neben den Skills der digitalen Welt auch viele Softskills beherrschen. Eigenorganisation, Selbstmotivation, sind z.B. Fähigkeiten die Mitarbeiter in der heutigen Zeit benötigen.
- Unsicherheit schafft Ängste für viele Arbeitnehmer. Wie kann man für die Arbeitnehmer wieder mehr Sicherheit schaffen?

4.17 War of Talents

In manchen Branchen gibt es zu **wenige qualifizierte und ausgebildete Fachkräfte**. Die Unternehmen stehen im Wettbewerb um die „Besten Köpfe“. Viele Arbeitnehmer entscheiden sich für oder gegen einen Arbeitsplatz aufgrund des angebotenen Betriebsklimas und der technologischen Ausstattung. Wer es gewohnt ist, mit Smartphones immer und überall zu arbeiten, möchte nicht in einem Unternehmen sein, das seinen Mitarbeitern keine sozialen Plattformen zum Austausch und keine flexiblen Möglichkeiten zum Arbeiten zur Verfügung stellt. Technologieunternehmen wie Google und Microsoft haben diesen Trend erkannt und gestalten ihre Arbeitsmodelle, aber auch Büroräumlichkeiten sowie Mitarbeitern zur Verfügung gestellte Infrastruktur und Geräte entsprechend.



- Die Unternehmen, die attraktiv für die besten Köpfe sein wollen, müssen auch ein attraktives Unternehmensumfeld schaffen.
- Firmen müssen Mitarbeiter Tools zur Verfügung stellen, die sie auch aus dem privaten Umfeld gewohnt sind. Wenn diese das nicht tun, haben sie es schwer Mitarbeiter zu finden, denn diese setzen ein modernes Arbeitsumfeld voraus.

4.18 Führen in der digitalen Welt

Für Manager ist es heute schwierig. Früher war der Manager in der Nähe des Mitarbeiters, Das Management konnte die Mitarbeiter immer unter „Kontrolle“ haben. Heute benötigen Manager **Vertrauen**. Es lässt sich schwer kontrollieren, wieviel ein Mitarbeiter arbeitet, der nicht nebenan am Schreibtisch sitzt, sondern flexible Arbeitszeiten hat, und unterwegs und im Kaffeehaus arbeitet. Mitarbeiterführung ist in der heutigen Zeit etwas Anderes als noch vor 20 Jahren. Manager benötigen neue Kompetenzen, müssen coachen und über Zielerreichung steuern.



- Manager müssen auf das Führen in der digitalen Welt vorbereitet werden.
- Manager müssen ihren Mitarbeitern ein hohes Maß an Vertrauen entgegenbringen.
- Coaching ist ein wichtiges Management Instrument.
- Der Manager misst den Beitrag des Mitarbeiters über qualitative und quantitative Ziele, nicht über im Büro verbrachte Arbeitszeit.

4.19 Veränderung von Jobs

Es gibt derzeit ähnliche Horrorszenarien, die wir bereits aus vergangenen Jahrhunderten kennen. Bereits 2013 wurde in einer dunklen Prognose von Carl Benedikt Frey und Michael A. Osborne³ vorausgesagt, dass **fast 50% aller Jobs durch die Digitalisierung wegfallen werden**. Die Prognose mag richtig sein, denn die Automatisierung hat mittlerweile auch 100% aller Schrankenwärter bei der Eisenbahn obsolet gemacht, dafür wurden in anderen Branchen mehr Jobs geschaffen als weggefallen sind. Wir tendieren daher eher zur Ansicht, dass es erneut zu Umbrüchen kommen wird, bei denen **weniger qualifizierte Jobs durch die Automatisierung ersetzt werden, jedoch neue Jobs in anderen Bereichen geschaffen werden**. Die Jobbilder sind also nach wie vor einem rasanten Umbruch unterworfen.



- Qualifizierung ist das wichtigste Kriterium für einen Arbeitnehmer.
- Die Digitalisierung wird **niedrigqualifizierte** Jobs eliminieren.
- Da die Entwicklung rasant ist, bleibt eine ständige Weiterbildung unumgänglich, um am Ball bleiben zu können.
- Da sich vor allem ältere Arbeitnehmer schwer mit Veränderungen tun, aber erwartet wird, dass die Arbeitnehmer immer länger arbeiten, müssen hier entsprechende Angebote geschaffen werden.

³ http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

4.2 Wirtschaft



Die Digitalisierung der Wirtschaft hat längst begonnen und es gibt weitreichende Veränderungen dadurch. „Disruptive Change“ ist das Schlagwort. Ein Unternehmen wie Uber besitzt kein einziges Fahrzeug, und macht Taxiunternehmen weltweit zu schaffen. Airbnb besitzt kein einziges Bett, konkurriert aber Hotels weltweit. Apple ist der größte Musikanbieter weltweit – und

Amazon der größte Supermarkt. Die Geschäftsmodelle verändern sich also hier dramatisch. Das größte Problem von Anbietern ist es ihr Geschäft für die Kundschaft „sichtbar“ zu machen.

Bedenklich ist aber, dass laut einer Studie von Crisp Research nur 7% der Geschäftsführer deutscher Unternehmen sich fit im digitalen Bereich fühlen. [71% der 503 Geschäftsführer stufen sich als „Digital Beginner“⁴](#) ein. Diese Zahlen sollten beunruhigen – es gibt erheblichen Aufholbedarf in den Chefetagen. Die Zahlen in Österreich werden diesbezüglich sicherlich nicht anders ausfallen.

4.2.1 Steuergesetzgebung

Die Steuergesetzgebung in Europa ist ein wichtiges Thema. Derzeit gibt es innerhalb Europas keine einheitliche Steuergesetzgebung. Die Mitgliedsstaaten legen die Steuern selbst fest.

Steuern sind auch ein Mittel um Anreize von Unternehmen zu setzen sich in einem Land niederzulassen. Wenn man Also im Land A weniger Steuer bezahlt, dann wird ein Unternehmen lieber ins Land A ziehen und nicht ins Land B.

Bei physischen Gütern ist aber die Wahl eines Unternehmensstandortes nicht ganz so einfach. Denn wenn ich Möbel kaufen möchte, dann benötige ich z.B. den Möbelmarkt in meinem Land. Dann werden Umsätze und nachfolgend hoffentlich auch die Gewinne im Land generiert, wo auch die Konsumenten leben.

⁴ <http://www.netzpiloten.de/digitalkompetenzen-hundefutter-transformation-unternehmen/>

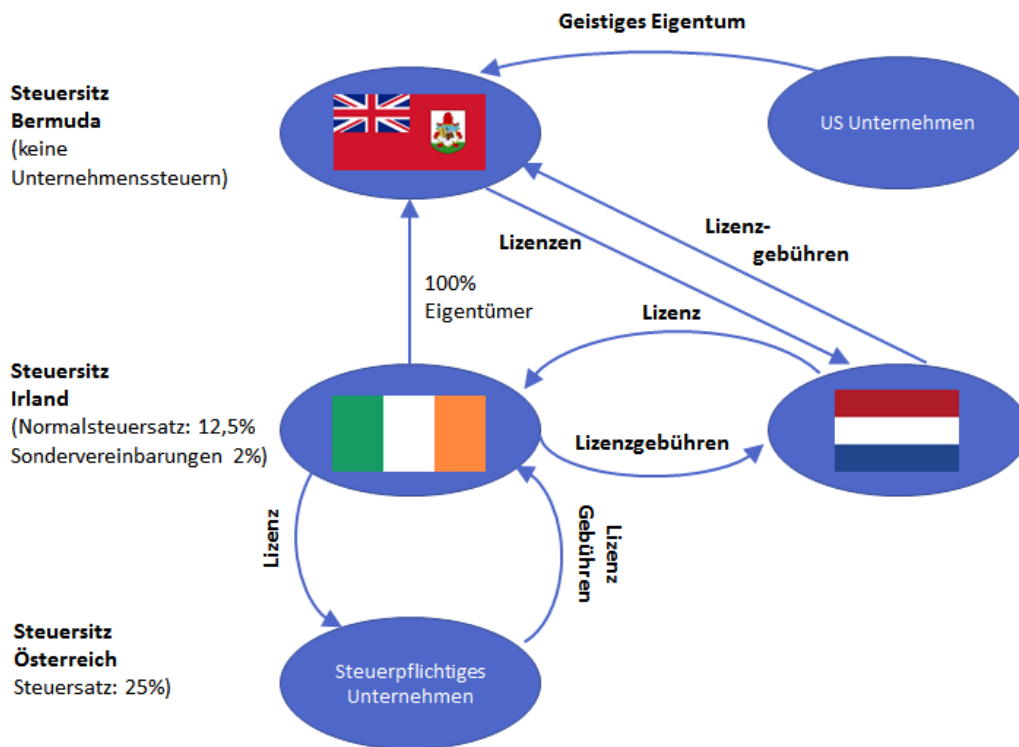
In der digitalisierten Welt ist aber diese Bindung an physische Standorte nicht mehr notwendig. Ein Stück Software, ein Musikstück, ein Film, Fotos, Bücher, etc. können eigentlich überall auf der Welt angeboten werden. Es gibt keine Verbindung mehr zwischen Ort des Angebotes und dem Ort wo der Konsument lebt.

In diesem Fall kann also ein Unternehmen auch frei wählen wo es seinen Firmensitz hat. Es wählt also das Land in dem es am wenigsten Steuern zahlt. Das ist vollkommen klar.

Nun ist es innerhalb der Europäischen Union so, dass die einzelnen Mitgliedsstaaten in Konkurrenz zueinander stehen. Nehmen wir an, das Land A verlangt 25% Steuer vom Gewinn eines Unternehmens. Das Land B möchte den Anbieter dazu bewegen, dass es seinen Hauptsitz in sein Land verlegt - und bietet daher 10% Steuersatz an. Das Land C meint es sei besser noch ein wenig zu bekommen statt gar nichts - und bietet 5% - und das nächste Land bietet dann 2,5%. Genau das passiert momentan innerhalb der EU. Die Paradebeispiele solcher Länder sind Luxemburg und Irland. Das Problem an diesen Niedrigsteuerregelungen ist, dass sie Ausnahmen sind. Also der Fleischhauer ums Eck zahlt nach wie vor den normalen Steuersatz, nur die großen dicken fetten Fische werden bevorzugt behandelt.

Falls sich jemand schon einmal gefragt hat, warum sich die großen Technologiekonzerne gerade Irland oder Luxemburg für Ihre Europazentrale ausgesucht haben, dann hat man hier die Erklärung gefunden, es ist nicht wegen der guten Luft in Irland und auch nicht wegen des guten Essens in Luxemburg.

Zusätzlich gibt und gab es eine Reihe von Sonderregelungen die Unternehmen die Möglichkeiten gibt überhaupt keine Unternehmenssteuern abzuführen. Eine beliebte Konstruktion ist der „Double Irish with a Dutch Sandwich“:



Nehmen wir beispielsweise einen großen US Technologiekonzern, der in Österreich seine Produkte vertreibt.

Der Konzern gründet zwei Irische Unternehmen. Das erste ist ein Unternehmen mit Steuersitz in Irland. Das zweite Unternehmen ist ein Unternehmen auf den Bermudas. Das erlaubt eine Besonderheit im Irischen Steuerrecht. Wenn das Unternehmen operativ nicht in Irland tätig ist, kann es auch im Ausland besteuert werden. Hier wird deswegen die Bermudas gewählt, weil es dort keine Unternehmenssteuern gibt. Auf den Bermudas erwirtschaftete Gewinne bleiben also vollkommen steuerfrei.

Der Konzern überträgt nun die Patentrechte oder Markenrechte oder sonstiges geistiges Eigentum an dieses neu gegründete Unternehmen auf den Bermudas. Das Unternehmen in Bermuda räumt einem ebenfalls neu gegründeten Unternehmen in den Niederlanden Rechte (eine Lizenz) ein die Markenrechte oder das geistige Eigentum, dass sich nun im Eigentum des Unternehmens auf Bermuda befindet zu nutzen.

Das Niederländische Unternehmen räumt nun dem ersten neuen Irischen Unternehmen die gleichen Rechte ein. Das Irische Unternehmen zahlt nun Lizenzgebühren an das Niederländische Unternehmen. Diese Konstruktion ist deswegen notwendig, weil bei einer direkten Überweisung an die Firma auf den Bermudas Quellensteuer anfallen würde. Durch ein Abkommen zwischen den Niederlande und Irland werden Lizenzgebühren von dieser Steuerpflicht ausgenommen.

Das Irische Unternehmen wiederum überlässt diese Rechte dem Österreichischen Unternehmen. Das Österreichische Unternehmen wiederum muss als Gegenleistung für diese Rechte Lizenzgebühren an das Irische Unternehmen abführen. Diese Lizenzkosten sind dann im Regelfall so hoch wie die Gewinne in Österreich wären. Dadurch werden die Gewinne in Österreich vollständig durch die Lizenzgebühren aufgeessen. Es sind daher in Österreich leider keine Gewinne zu versteuern. Die Niederlassung in Österreich nagt ja am Hungertuch.

Damit ist der Gewinn aus Österreich vollkommen unversteuert auf den Bermudas gelandet. Ebenso aus allen anderen Europäischen Ländern. Weder der Fiskus in Österreich, noch der in Irland, Niederlanden haben Steuern gesehen. Und im Steuerparadies Bermudas gibt es ohnehin keine Steuern.

Die neue Einrichtung eines solchen Konstrukts ist seit 2015 nicht mehr möglich. Denn in Irland eingerichtete Unternehmen müssen nun auch ihren Steuersitz in Irland haben. Es gibt aber für Unternehmen die diese Konstruktion bereits nutzen großzügige Übergangsfristen bis 2020.

Aus Sicht der Europäischen Bürger und Konsumenten sind diese Steuerpraktiken abzulehnen, denn warum sollten es große Unternehmen richten können, und keine Steuern auf ihre Gewinne zahlen, während Arbeitnehmer ihre Steuer bereits vom Arbeitgeber abgezogen bekommen. Der Grenzsteuersatz liegt in Österreich immerhin jetzt bei 55%.

Aber auch aus Sicht der lokalen Unternehmen und der Österreichischen Wirtschaft führt eine derartige Besteuerung zu einer Wettbewerbsverzerrung. Der lokale Wirtschaftstreibende führt brav seine Steuern ab. Er konkurriert aber mit Unternehmen die ungleich behandelt werden. Die ungleiche Besteuerung ist wettbewerbsverzerrend.

Die Europäischen Staaten (aber auch die USA) haben nichts davon. Einzig durch den Steuerwettbewerb unter den einzelnen EU Mitgliedstaaten bleiben ein paar Brösel in einem der Länder (Irland, Luxemburg) hängen. Aus einer gesamtheitlichen Sicht ist das aber ein volkswirtschaftlicher Irrsinn der hier angestellt wird. Alle Europäischen Staaten fallen um die Steuerzahlungen um, nur um ein paar wenige Arbeitsplätze für (relativ kleine) Europahauptquartiere in eines der Mitgliedsländer zu zerren.

Die Europäische Union ist dagegen auch machtlos, denn die Steuergesetzgebung fällt in die Kompetenz der Mitgliedsländer. Einzige vernünftige Lösung um solche Stilblüten zu lösen wäre eine Fiskalunion zusätzlich zur Währungsunion.

4.2.2 Cloud-Computing



IT in Unternehmen ist ein sehr komplexes und kostenintensives Thema. Jedes größere Unternehmen hat eine eigene IT Abteilung die seit vielen Jahren hoch individualisierte und maßgeschneiderte Lösungen für ihr Unternehmen bauen. Das Problem dieser Legacy Systeme ist, dass jedes Upgrade – jede Veränderung am System hochkomplex aufwändig und personalintensiv ist. IT

wird in diesen Bereichen oft zum Wettbewerbsnachteil, da in der sich immer rascher entwickelnden Welt Flexibilität ein entscheidender Wettbewerbsvorteil ist.

Cloud-Computing verspricht hier Abhilfe. Die Idee von Cloud-Computing ist es, generische, standardisierte IT Lösungen für Kunden anzubieten, die nicht einmal eine lokale IT benötigen. Hochgradig standardisierte Services werden aus einem Cloud Rechenzentrum heraus angeboten.

Dieses Cloud Rechenzentrum kann aufgrund seiner schieren Größe Kosteneinsparungen im Bereich von Hardware, Wartung, Stromversorgung lukrieren, die für einen normalen Kunden/Anwender undenkbar wären. Automatische Provisionierung von Systemressourcen – und hochgradige Automatisierung reduzieren vor allem die Personalkosten weiter.

Durch die Flexibilität der Einführung solcher Systeme (keine Hardware, keine großen Implementierungsprojekte) ist der Kunde wesentlich flexibler. Die o.g. Kostenvorteile generieren zusätzlich Druck auf die lokale IT, diese Dienste zu nutzen.

Cloud-Computing ist vergleichbar damit, dass früher jede Fabrik ihr eigenes Kraftwerk hatte und Strom erzeugt hat. Heute kommt niemand mehr auf diese Idee. Es ist viel effizienter, das standardisierte Produkt Strom von einem dafür spezialisierten Provider zu beziehen. Ein ähnlicher Prozess ist derzeit in der IT zu beobachten.

Problematisch bei Cloud Systemen wird vor allem das Thema der Datenspeicherung gesehen. Kann der Cloud Provider garantieren, dass niemand unberechtigter auf die Daten zugreifen kann? Das bezieht sich vor allem auch auf Geheimdienste. Denn kein Kunde möchte seine kritischen Daten in falschen (z.B. auch industriespionierenden) Händen wissen.

Ein besonderer Aspekt ist hier der US Amerikanische **FISCUS Foreign Intelligence Surveillance Court** ^[Obj.] kann dieses Gericht sogenannte „gag orders“ ausstellen. Dabei wird ein Unternehmen (z.B. ein Cloud Provider) zur Herausgabe von Kundendaten verpflichtet, der betroffene Kunde darf dabei aber nicht informiert werden. Besonders europäische Firmenkunden mit heiklen Kundendaten (z.B. Banken, Pharmaunternehmen, Gesundheitseinrichtungen, ...) stoßen sich an dieser Regelung, da sie in diesem Falle nicht einmal informiert würden, wenn die US Regierung Daten ihrer Kunden anzapft. Sie können sich daher auch gegen einen derartigen Zugriff nicht wehren, weil das Rechtssystem ausgeschaltet wurde.

US Cloud Service Provider bzw. europäische Unternehmen mit Niederlassungen in den USA befinden sich in einer Zwickmühle. Auf der einen Seite [verlangen US Gesetzeshüter Zugriff auf Daten, die sich in EU Rechenzentren befinden](#).⁵ Auf der anderen Seite gibt es geltende lokale Gesetze die den Zugriff auf solche Daten regeln. Aus unserer Sicht darf der Zugriff auf Daten, die sich in der EU befinden, nur über Amtshilfeersuchen und Prüfung durch ein lokales europäisches Gericht erteilt werden.

⁵ http://www.theregister.co.uk/2014/09/23/microsoft_vs_the_long_arm_of_us_law/

Ein weiteres Problem für die Nutzung von Cloud Technologien sind die **unterschiedlichen regulatorischen Anforderungen** von regulierten Industrien. Eine Vereinheitlichung dieser Richtlinien in den EU Mitgliedsstaaten würde die Nutzung von Cloud Technologien für diese Institutionen erheblich vereinfachen.



- Aufklärung der Firmen über Nutzen und Risiken von Cloud Technologien.
- Veränderungen für Arbeitnehmer durch den Einsatz von Cloud Technologien (z.B. IT Administrator). Die Jobrollen verändern sich.
- Sicherheit für den Schutz der Daten der Kunden in den Cloud Rechenzentren
- Gesetzliche und regulatorische Regelungen für Cloud Technologien.

4.2.3 Produktion und Industrie 4.0



Auch die Wirtschaft ist durch die Digitalisierung einer starken Veränderung unterworfen. Die Auslagerung von Produktionsprozessen in Billiglohnländer wurde erst durch neue, schnelle Kommunikation möglich. Markenunternehmen fokussieren sich zunehmend nur noch auf die Entwicklung, gefertigt wird ausschließlich in Fernost.

Um im Produktionsbereich in Österreich und Europa wettbewerbsfähig sein zu können, müssen Unternehmen die Vorteile der Digitalisierung des Produktionsprozesses optimal nutzen, oder sich auf die Herstellung von Produkten verlegen, für die größeres Know-how notwendig ist. In diesem Bereich haben wir jedoch noch großen Aufholbedarf.

Im Fokus von Industrie 4.0 steht die Maschine zu Maschine Kommunikation und die Möglichkeit, Fertigungsprozesse möglichst vollständig zu digitalisieren. Das spart Geld, und Arbeitszeit – und daher auch Kosten und ermöglicht eine flexible Großserienproduktion bis hin zur „mass-customization“.

4.2.4 3D Printing

Im Zuge des Produktionsprozesses gibt es die neue Technologie des 3D Drucks. 3D Druck“. Diese Technik ermöglicht es auch, Einzelanfertigungen von z.B. Ersatzteilen günstig herzustellen.

Die Technologie des 3D Drucks hat massive Vorteile – birgt aber auch Gefahren wie die erfolgreiche Fertigung von Waffen, aber auch die 3D Modelle der TSA Schlüsseln, die mittlerweile im Internet verfügbar sind zeigen.



- Wie kann die 3D Printing Technologie genutzt werden um lokale Unternehmen zu stärken?
- Sicherheitsfragen die durch 3D Druck aufgeworfen werden (Druck von Waffen, Herstellung von (TSA Nachschlüsseln, ...)

4.2.5 Internet of Things (IoT)

Das "Internet of Things" (IoT) ermöglicht es, beinahe alle Arten von Geräten oder Anlagen mit einer digitalen Schnittstelle zu versehen und mit deren Hilfe den aktuellen Zustand – beispielsweise hinsichtlich notwendiger Wartung – abzufragen. Dadurch kann frühzeitig korrigierend eingegriffen werden, noch bevor ein Fehlerfall eintritt. Die dabei erfassten Daten können nicht nur zur Steuerung von Prozessen verwendet werden, sondern liefern auch die Grundlage für Analysen aller Art. Datenschutzrechtlich unproblematisch ist das beim Einsatz von IoT im Bereich von Produktionsprozessen und Industrieanlagen.

Die "Digitalisierung" und Vernetzung von klassischen Gerätschaften wirft bedeutsame Fragen nach der **Sicherheit** auf. Im Internet ist mittlerweile mehrfach dokumentiert, dass auf Industrieanlagen ungeschützt über das Internet zugegriffen werden kann und diese so gesteuert werden können. Hier ist bei den Herstellern und Betreibern solcher Anlagen noch erheblicher Aufklärungsbedarf über die Risiken gegeben.

Die Sammlung von Daten über IoT Systeme kann problematisch werden, wenn diese Daten Rückschlüsse auf Personen oder auch geheim zu haltende Firmendaten erlauben. Der zeitliche Stromverlauf oder Ein-/Ausschaltintervalle, oder andere Sensordaten eines Geräts erlauben es, auf seine Bedienung zurück zu schließen und damit letztlich die Menschen zu überwachen, die dieses Gerät bedienen/besitzen. Eine Anonymisierung solcher Daten ist oft nicht vollständig möglich. Bedenklich scheint z.B. die Übernahme des Home Automation Herstellers „Nest“ durch Google. Eine Vernetzung der Daten aus der Google Suche mit den Sensoren der Hausautomatisierung erscheint

datenschutzrechtlich mehr als bedenklich. Es bedarf klaren Regelungen, wer und wie die Daten benutzen und ggf. weitergeben darf. Der Nutzer benötigt das Recht, genau zu wissen, welche Informationen gesammelt werden, wozu sie verwendet werden – und er muss auch das Recht haben auf der vollständigen Löschung der gesammelten Daten zu bestehen.

Es bedarf auch eine Regelung, wer für den Fall eines Datenverlustes in welcher Höhe für den entstandenen Schaden verantwortlich ist. Die Strafen müssen so gestaltet sein, dass es für das Unternehmen kosteneffizienter ist, in Sicherheitsmaßnahmen zu investieren, als ein Datenleck in Kauf zu nehmen.

Ebenso ist beispielsweise der **Einsatz von IoT im Versicherungsbereich** problematisch, wenn z.B. Automobile regelmäßig ihre Nutzungsdaten an eine Versicherung liefern und diese dann ihre Tarife entsprechend anpasst. Es kann so dazu führen, dass Personen die viel unterwegs sind, gar nicht mehr von Versicherungen akzeptiert werden, weil sie ein zu großes Risiko darstellen. Das Versicherungssystem lebt von der Solidarisierung des Risikos. Wenn dieses nicht mehr möglich ist, funktioniert das Versicherungssystem generell nicht mehr. Ebenso wäre die Verwendung dieser Daten durch Behörden problematisch (z.B. automatische Strafmandate bei Überschreitung der Höchstgeschwindigkeit).

4.2.6 Big Data & Datenhandel

Big Data ermöglicht es, große Datenmengen auszuwerten und die daraus gewonnenen Erkenntnisse gewinnbringend zum Beispiel im Vertrieb und Marketing zu nutzen. Es werden daher meist Verhaltens- und Nutzungsprofile der Benutzer erstellt.

Diese Funktion ist sehr nutzbringend in verschiedenen Bereichen – und Unternehmen können hier Dinge lernen, die ohne die Nutzung von Big Data vollkommen unmöglich wären. Ein Beispiel ist die Auswertung von Social Media Kommentaren zu Produkten oder Marken. Dabei kann eine Firma ableiten, wie ihre Produkte angenommen werden und welche Kritikpunkte es gibt.

Datenschutzrechtlich problematisch ist vor allem, wenn personenbezogene Daten aus unterschiedlichsten Quellen und ohne Möglichkeit zur Beeinflussung durch die Betroffenen zusammengezogen und ausgewertet werden.

Die größten Datensammler weltweit sind Werbeunternehmen wie Facebook und Google. Sie sammeln Daten über ihre Nutzer nicht nur auf den eigenen Webseiten, sondern über ihre Einbindung auf einem Großteil der Websites über z.B. Google Analytics oder Facebook Social Plugins. Der Nutzer kann sich dieser Verfolgung nicht entziehen.

Aber auch Unternehmen wie die Österreichische Post AG gehören zu den Datensammlern. Postmitarbeiter sammeln auch Informationen wie etwa wie viele Personen in einem Haushalt leben, wie hoch das Haushaltseinkommen ist, ob man Haustiere hat und vieles anderes mehr.

4.2.7 Online Vertriebswege

Der Vertrieb erfolgt vermehrt online, sei es über Business-to-Business (B2B) Kommunikation direkt zwischen den Warensystemen der Händler oder aber im direkten Kundenvertrieb (B2C) über Online-Shops, die den klassischen Ladengeschäften immer stärker Konkurrenz machen. Der Wettbewerb sitzt also oft nicht mehr im Geschäft ums Eck, sondern vielleicht in China. Große Anbieter wie Amazon oder Rakuten haben hier den Vorteil des so genannten „Long Tails“, sie verfügen über ein riesiges Angebot mit entsprechendem Lagerstand, mit dem heimische Anbieter in vielen Fällen nicht mithalten können.

Das größte Problem für lokale Händler scheint aber die Ungleichbehandlung bezüglich **Steuergesetzgebung** zu sein. Lokale Händler müssen ihre Gewinne ordentlich versteuern, während ihre großen Konkurrenten „es sich richten“ können. Über verschiedene Steuerdeals mit Regierungen bis hin zu Finanz-Konstrukten, wie dem „Double Irish with a Dutch Sandwich“, mit dem die Unternehmensgewinne legal in Steueroasen transferiert werden können. Wichtig wäre hier die Herstellung eines „level playing field“ (Wettbewerbsgleichheit) für alle Beteiligten.

Ein weiteres Problem für die lokalen Händler ist die Umgehung von arbeitsrechtlichen Vorschriften für Paketboten und Transporteure, aber auch Mitarbeitern in Logistikzentren der großen Versandhändler. Würden z.B. die Paketboten nach geltendem **Arbeitsrecht** behandelt, würden die Kosten für den Versand der Pakete sicherlich höher ausfallen, und lokale Anbieter könnten besser mit dem Versandhandel mithalten.



Forderung der Digital Society:

- Es muss eine Gleichbehandlung in der Steuergesetzgebung hergestellt werden. Es kann nicht angehen, dass Konzerne ihre Gewinne in Steueroasen verschieben, während lokale Anbieter ihre Gewinnsteuern normal bezahlen. (Stichwort: Double Irish with a Dutch Sandwich). (EU)

4.2.8 Digitale Werbung und Marketing

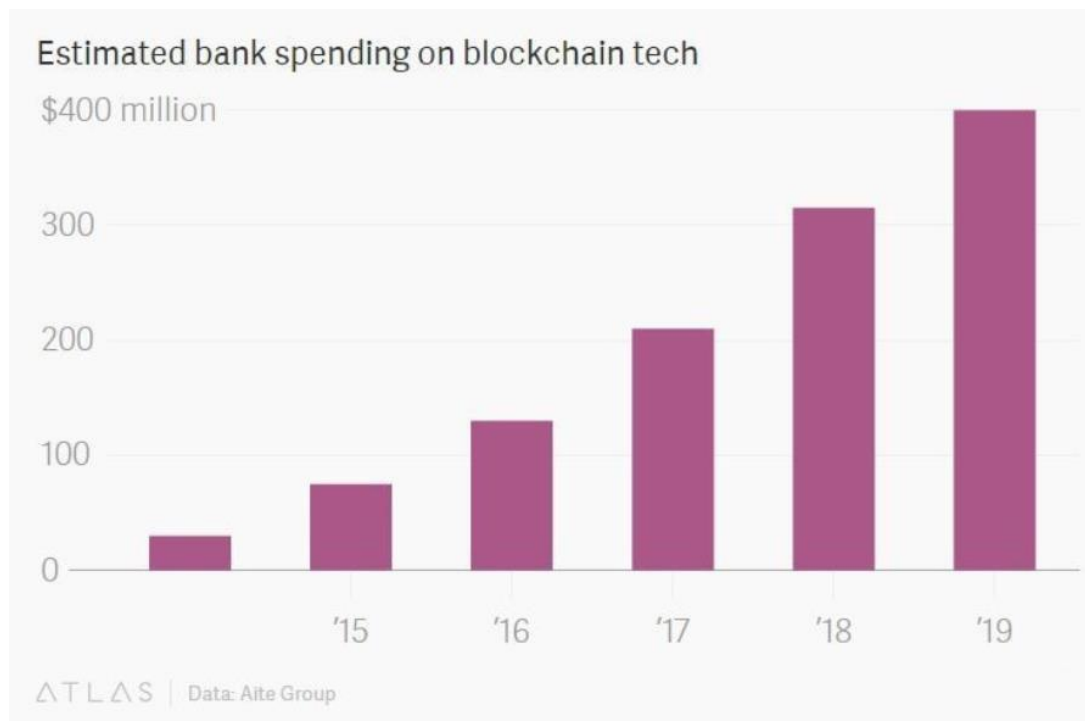
Facebook und Google haben mittlerweile die Stelle übernommen, die früher Fernsehen und Zeitungen zukam. Die klassischen Werbeträger verlieren jährlich an Umsatz, dafür gewinnen ihre digitalen Counterparts jährlich hinzu.

Datenschutz wird da oft als störender Faktor gesehen, die Begehrlichkeiten nach personengenau zugeschnittener Werbung sind hoch. Die Herausgabe von persönlichen Daten wird aber zunehmend von den Konsumierenden als kritisch gesehen. Ein starker **Datenschutz der Kundendaten** wird zunehmend zu einem Entscheidungsgrund und damit zu einem Wettbewerbsvorteil.

4.2.9 Zahlungsverkehr

Neue Zahlungsanbieter wie PayPal, Sofortüberweisung, etc. jagen den Banken Marktanteile im Zahlungsverkehr ab. Neue Währungen wie Bitcoin können Bargeld ersetzen.

Auch im Bereich des klassischen Zahlungsverkehrs gibt es massive Umbrüche. Die Banken kämpfen hier aus ihren traditionellen Positionen sehr damit, wie sie mit diesen Veränderungen umgehen sollen – und überlassen dieses Feld oft kampflos dem Wettbewerb. Technologien wie die von Bitcoin genutzte Blockchain Technologie haben das Zeug große Banken für die Abrechnung untereinander (Trusted Intermediary) obsolet zu machen und die Kosten dafür dramatisch zu senken. Banken investieren daher selbst in diese Technologie in der Hoffnung zumindest einen Teil des Geschäfts zu retten.



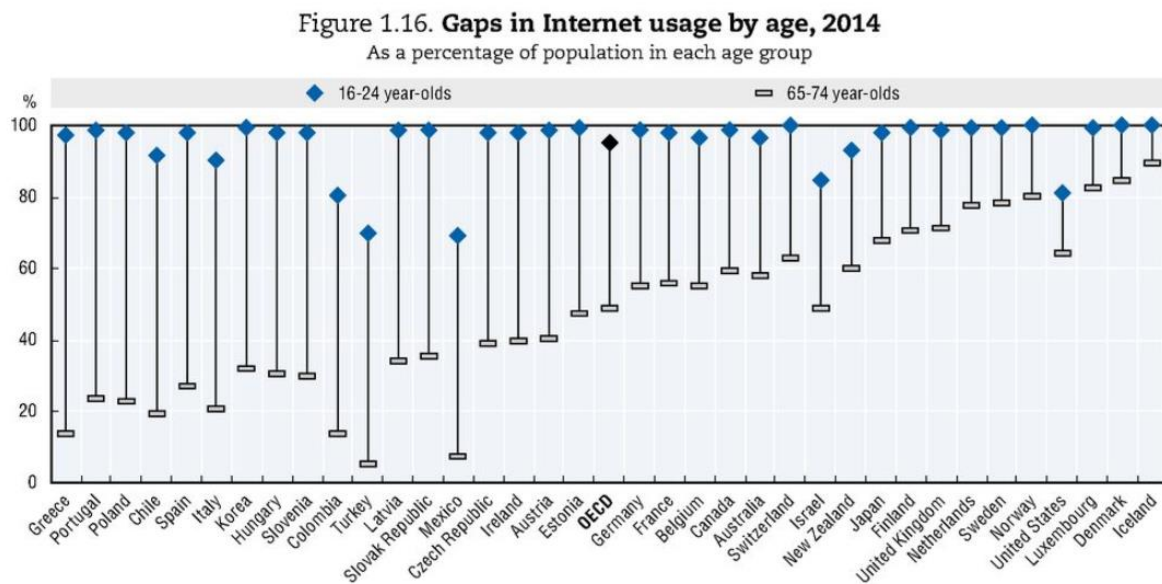
4.3 Privatleben & Familie



Die Digitalisierung hat auch massive Auswirkungen auf unser Privatleben. Es öffnet sich aber auch eine ganz spezielle Kluft zwischen den Generationen (Großeltern, Eltern, Kinder). Auch gefährdet die Digitalisierung unseres Privatlebens die Privatsphäre der gesamten Familie. Und viele der Betroffenen ahnen die Gefahren nicht einmal – oder sind ihnen gegenüber gleichgültig.

4.3.1 Digital Divide / Digitale Kluft

Innerhalb der OECD liegt Österreich im Bereich der Digital Divide im Jahre 2014 laut einer OeCD Studie im unteren Mittelfeld. Nur etwa 40% der 65-74 jährigen verwenden das Internet. Dagegen liegt die Verwendung bei den jugendlichen (16-24 Jahre nahe bei 100%).⁶



⁶ http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2015_9789264232440-en#page81

Diese Studie zeigt auf, dass Österreich gerade bei den Senioren einen starken Aufholbedarf hat. In Island liegt beispielsweise der Anteil von Senioren, die das Internet aktiv nutzen, bereits bei rund 90%

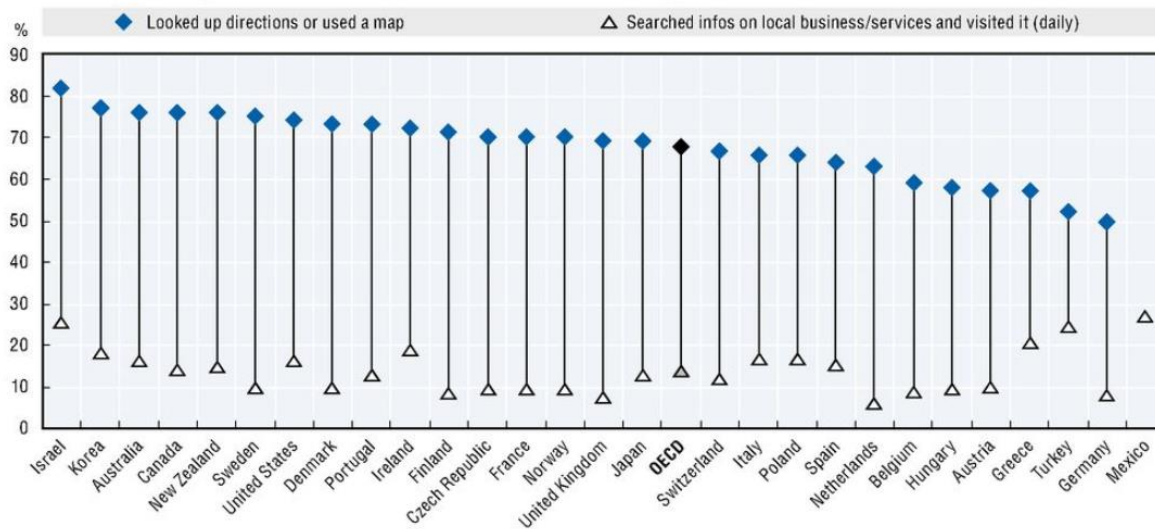
4.3.2 Smartphones & Devices

Auf unserem Smartphone tragen wir mittlerweile unser Leben mit uns herum. Wenn es gestohlen wird, ist das ein echtes Problem für uns. Das Smartphone verwaltet alle unsere Kontakte, unseren Kalender, wir tragen Kopien der wichtigsten Dokumente mit uns digital herum, es ersetzt die Kundenkarten beim Einkauf. Es ist ein Ortungsgerät, das uns sagt, wo wir gerade sind, das uns aber auch sagen kann, wo sich andere Menschen gerade befinden, wo sich unsere Kinder herumtreiben. Es ist ein Navigationssystem, das uns sagt, wohin wir wie mit dem Auto fahren. Und natürlich ist es auch Fotoapparat und Videokamera. Es ist unser wichtigstes Kommunikationsgerät, um mit unserer Familie und unseren Freunden in Kontakt zu bleiben. Telefoniert wird damit aber immer weniger, immer mehr findet solche private Kommunikation über soziale Netzwerke wie Facebook, WhatsApp oder Skype statt.

Da so eine Vielzahl an sensiblen Daten auf diesem Gerät gespeichert sind, sollten sowohl die Inhalte am Gerät verschlüsselt sein (für den Fall, dass es verloren geht oder gestohlen wird), als auch die Kommunikation des Gerätes mit Diensten im Netz nicht abhörbar sein. Dabei sollte das vom Gerät bzw. der Software als Default passieren und daher für den Benutzer transparent sein. Denn Nutzer sind im Allgemeinen nicht dazu in der Lage, komplexe Konfigurationen, die derzeit dafür notwendig sind, auszuführen.

Österreich liegt aber auch bei der Verwendung von Diensten (Kartendienste, Suche nach lokalen Geschäften) auf dem Smartphone eher im unteren Bereich:

Figure 1.18. **Smartphone use of selected geo-location services, 2013**



Notes: No data available for Chile, Estonia, Iceland, Luxembourg, Slovak Republic, Slovenia. The sample covers private smartphone users who use the Internet in general.

Source: Our Mobile Planet, 2013.

4.3.3 Wearables

(text fehlt noch)

4.3.4 Fotografie und Video

Dass Fotoapparate keine Filme mehr benötigen, weiß mittlerweile auch schon die ältere Generation. Jedes Handy ist ein Fotoapparat und eine Videokamera. Handys laden geschossene Fotos automatisch in die "Cloud – speichern, wo sie geschossen wurden, und veröffentlichen sie in sozialen Medien. Usability ist das Schlüsselwort des großen Erfolges. Traditionelle Fotoapparate-Hersteller wie Nikon und Canon kämpfen mit der Handy-Konkurrenz und erweitern Fotoapparate um Video- und Netzwerk-Funktionen.

Die Digitale Fotografie und vor allem die Vernetzung mit Sozialen Medien hat jedoch auch seine Tücken. So landen auch oft Fotos, von denen man es vielleicht nicht unbedingt möchte, im Internet. Besonders Jugendliche machen sich wenig Sorgen darum, wer diese Bilder sehen könnte.

Viele Nutzer machen sich auch keine Gedanken um Nutzungsbedingungen von diversen Online Plattformen. So geht das Nutzungsrecht an hochgeladenen Fotos auf Facebook über – und Facebook kann damit im Grunde genommen tun und lassen was es will.

Auch das Urheberrecht ist in vielen Bereichen problematisch. Denn es ist für einen Anwender oft schwer zu entscheiden, ob ein Foto urheberrechtlich geschützt ist. Verwendet man ein Foto auf einer Website oder in Facebook kann das oft teuer kommen, wenn der Rechteinhaber eine Rechnung für die Verwendung des Fotos schickt.

4.3.5 Medienkonsum

Am deutlichsten wird die Revolution im Privatleben derzeit im Mediensektor sichtbar.

4.3.5.1 Fernsehen und Video

Fernsehen im traditionellen Sinne wird von der Jugend kaum mehr wahrgenommen. Fernsehen, aber auch CDs und DVDs werden zunehmend durch Streaming und On-Demand-Downloads ersetzt. Dass man zu einer bestimmten Zeit vor der "Kiste" sitzen muss, um eine Sendung zu sehen, kennen Jugendliche nicht mehr (Netflix, TVThek, Horizon Go). Die Zeit, die Zuseher für traditionelles Fernsehen verwenden, nimmt laut einer Studie der Nielssen Gruppe seit 2009 kontinuierlich ab.

Das klassische Fernsehen ist Regulierungen unterworfen. Es ist streng reguliert wie viel Werbung gesendet werden darf, oder welche Inhalte zu bestimmten Uhrzeiten gesendet werden können. Diesen Regulierungen sind die Konkurrenten YouTube und Netflix nicht unterworfen.

4.3.5.2 Radio und Podcasts

Auch das Radio verwendet mittlerweile als Transportmedium das Internet öfter als den Äther. Radiosender sind mittlerweile generell über Live-Streaming verfügbar. Ausgewählte Sendungen auch als Podcasts.

4.3.5.3 Print Medien

Zeitungen und Zeitschriften werden zum Premium-Produkt. Hochglanzmagazine, die Lifestyle vermitteln, haben noch guten Absatz – normale "News" verschafft man sich aber immer weniger auf Papier und immer mehr im Internet. Früher wurden Einnahmen für die Onlineauftritte in Zeitungen vor allem mit Banner Werbung finanziert. Wirklich einträglich war dieses Geschäft aber noch nie und es ist auch weiter rückläufig. Zeitungen versuchen diesem Trend mit s.g. Paywall zu begegnen. Man bekommt bestimmte Artikel nur mit einem Abonnement. Zeitungen versuchen aber auch durchzusetzen, dass Suchmaschinenanbieter für die Anzeige von Auszügen ihrer Artikel etwas bezahlen sollen (s.g. Leistungsschutzrecht^(OBJ)). Hier scheint es aber so zu sein, dass dem Verfechter dieser Lösung das Verständnis für die Funktion des Internets und von Suchmaschinen fehlt.

4.3.6 Einkaufen

Auch unser Einkaufsverhalten hat sich verändert. Wenn man etwas benötigt, sieht man schnell auf Amazon nach und bestellt Zutaten fürs Brotbacken genauso wie einen Ersatz für die kaputt gegangene Küchenmaschine oder Computerzubehör. Wer gerade nicht auf Amazon kauft, sieht zumindest auf Geizhals.at nach, wo man gerade das günstigste Gerät bekommen kann.

Sogar das Essen kommt zusehends "Online". Portale wie lieferservice.at oder mjam.net bieten an, Essen frisch aus der Umgebung nach Hause zustellen zu lassen, aber auch Lebensmittelhändler springen auf diesen Trend auf.

Besonders ältere oder gebrechliche Personen würden von Internet-Zustelldiensten profitieren, sind aber teilweise noch nicht in der Lage mit dem Medium Internet bzw. Computern im Allgemeinen umzugehen, und haben zu große Scheu davor. Hier könnten geförderte Schulungen bzw. Begleitung helfen, diese technischen Hürden abzubauen bzw. die Scheu zu reduzieren.

Und wenn man unterwegs ist, kann man am Smartphone besuchte Lokale oder Orte mit Foursquare, Tripadvisor oder Lokaltester.at bewerten oder davon profitieren, welche Bewertungen andere abgegeben haben und danach entscheiden, wo man sein Abendessen genießt.

4.3.7 Bankgeschäfte



Online ist mittlerweile der Standard bei Banken. Wenn man eine Bankfiliale besucht, weiß man mittlerweile oft nicht mehr, ob man wirklich in einer Bank ist. Beratung gibt es in manchen Banken kaum noch. Das Personal ist teilweise so schlecht geschult, dass man sich fragt, wie sie die Bankenprüfung überhaupt

bestehen konnten. Neue Szenarien wie Remote Beratung über z.B. Skype bieten Beratung nicht nur in der Filiale, sondern auch von zu Hause.

Banken sind in der Krise und versuchen ihre Ausgaben (vor allem Personal und Filialen) zu reduzieren. Der Kunde wird gedrängt, Telebanking zu nutzen, oder – falls er kein Internet hat – zu den Selbstbedienungsautomaten im Foyer der Banken zu gehen. Die Bank Austria denkt derzeit laut darüber nach, sich vom Privatkundengeschäft überhaupt zu trennen.

Neue Bezahlmethoden wie PayPal und BitCoin werden immer mehr. Unsere Mobiltelefone werden zu Geldbörsen und ersetzen viele der klassischen Bankomat- und Kreditkarten.

Manche Technologien, wie z.B. die NFC-Bezahlungsfunktion auf Bankkarten (Maestro bzw. Kreditkarten), werden von den Banken eingeführt, obwohl berechtigte Bedenken punkto **Sicherheit** existieren und entsprechende Angriffsvektoren auch aufgezeigt wurden.

Auch hier besteht eine **Einstiegshürde** für ältere Personengruppen. Diese quälen sich im Foyer mit Automaten ab, obwohl machen Tätigkeiten viel einfacher und bequemer von zu Hause aus lösbar wären. Entsprechende Schulungen für diese Gruppen wären auch im Interesse der Banken, um Kosten zu reduzieren und Kundenzufriedenheit zu erhöhen.

Bankgeschäfte werden aber auch manchmal nicht mehr sichtbar getätigt. So werden Kredite mittlerweile in Kaufprozesse integriert. Beim Kauf wird die Finanzierung gleich mit angeboten. Die Bank tritt nicht mehr in Erscheinung.

4.3.8 Automobil



Auch im Bereich der Mobilität gibt es rasante Umbrüche durch die Digitalisierung. Die neueste Entwicklung auf dem Gebiet sind **selbstfahrende Autos**. Die Digitalisierung der Fahrzeuge bietet enorme Komfortgewinne für den Fahrzeughalter. Mittlerweile kann man es sich z.B. kaum mehr vorstellen, wie es war, als die Autos noch keine Navigationssysteme hatten und wir mit Landkarten und Beifahrer

navigiert haben.

Es gibt in den Fahrzeugen mittlerweile kaum noch klassische Zündschlüssel. Diese wurden durch Funkschlüssel ersetzt. Der Fahrer muss den Schlüssel nicht mehr ins Zündschloss stecken – es reicht, wenn er ihn in seiner Jackentasche hat. Diese Systeme sind aber nachgewiesenermaßen nicht sicher. Hackern gelingt es mittlerweile Autos zu stehlen, deren Schlüssel sicher im Haus verwahrt ist. Die Funksignale des Schlüssels werden mittels eines Proxy zum Auto übertragen. Dieses lässt sich starten und auch ohne Schlüssel fahren, so lange bis der Motor wieder abgestellt wird. Der Besitzer hat also nichts falsch gemacht. Der Schlüssel war immer sicher verwahrt. Das neue Auto ist trotzdem weg, und die Versicherung macht oft Probleme, weil man dem Fahrzeuginhaber unterstellt, nicht achtsam genug gewesen zu sein.

Die gesamte Steuerung der Fahrzeuge erfolgt mittlerweile über elektronische Steuerungssysteme. Wie man beim VW Abgasskandal gesehen hat, steuert dieser Computer im Grunde genommen jeden einzelnen Wert des Motors, aber nicht nur diesen, auch Bremsen und Lenkung (Servo) werden mittlerweile per Computer gesteuert. Diese Steuerungssysteme sind aber keine abgeschotteten Systeme mehr – sie sind vernetzt. 2015 hatten es Hacker geschafft, über das UConnect System eines Jeeps die Kontrolle über das Fahrzeug zu erlangen – und zwar aus beliebiger Entfernung über das Internet – und das Fahrzeug letztendlich in den Graben zu fahren⁷. Glücklicherweise wurde dies in einem Versuch gezeigt und es saß ein Lenker hinter dem Steuer, der wusste was hier versucht wurde – denn sonst hätte das durchaus auch Leben kosten können.

⁷ <http://www.heise.de/security/meldung/Hacker-steuern-Jeep-Cherokee-fern-2756331.html>

Zusätzlich sammeln moderne Fahrzeuge so gut wie alle Daten über das Fahrzeug selbst, Damit ist auch der Datenschutz ein wichtiges Thema. Besonders wenn man die Daten des Fahrzeuges auch mit den Daten des Fahrers verknüpft (Big Data).



- Sicherheitsprobleme bei Fahrzeugen sind immanent – von gehackten Zündschlüsseln bis zur vollständigen Übernahme der Kontrolle eines Fahrzeuges. Ein PKW muss jedes Jahr zum „Pickerl“, aber die digitale Sicherheit der Fahrzeuge wird nicht geprüft.
- Auch Datenschutz wird in den Fahrzeugen ein immer wichtigeres Thema. Spätestens mit Einführung des e-Call Systems sind vollständige Bewegungsprofile der Fahrzeuge verfügbar.

4.4 Bildung & Forschung

4.4.1 Forschung und Innovation

4.4.1.1 Universitäten und Startups

In vielen Ländern sind die Universitäten der Keim des Fortschritts. Pulsierende Communities rund um diese Bildungseinrichtungen schaffen eine Atmosphäre in der sich Studenten wohl fühlen – und dazu führen, dass Studenten gerade diese Universität auswählen. Es gibt mittlerweile einen „War of Talent“ und wir müssen uns an diesem Kampf um die besten Köpfe beteiligen. Eine blühende Startup Szene bildet sich um diesen Keim.

Ausgezeichnete Universitäten sind also nicht nur eine Quelle für Unternehmen, die deren Abgänger als Arbeitnehmer benötigen, sondern auch ein Magnet für solche Unternehmen, gerade nach Österreich zu kommen. Investitionen in diese Universitäten sind also auch Wirtschaftsförderung.

Lieder liegen wir in Österreich im Rennen um die besten Unternehmen nur im Mittelfeld. Laut den „QS World University Rankings“⁸ schneiden die österreichischen Universitäten wie folgt ab:

RANK	UNIVERSITY	LOCATION	QS STARS
Overall Score ▼	Search for universities...		Show only
153 60.8	University of Vienna		
197 53.9	Vienna University of Technology		
295 42.6	Universität Innsbruck		
431-440	Karl-Franzens-Universitaet Graz		
551-600	Johannes Kepler University Linz		
701+	Alpen-Adria-Universitaet Klagenfurt		
701+	Paris Lodron University of Salzburg		

Die beiden Wiener Universitäten (Uni Wien und TU) liegen auf Platz 197 bzw. 295. Wenn man sich die Detailauswertung ansieht, so sieht man, dass der Grund dafür vor allem bei der Uni Wien in den Rahmenbedingungen als Arbeitgeber und bei der TU Wien in der mangelnden Internationalität des Lehrkörpers die Bewertung negativ beeinflussen.

⁸ <http://www.topuniversities.com>

4.4.12 Rahmenbedingungen für Unternehmertum

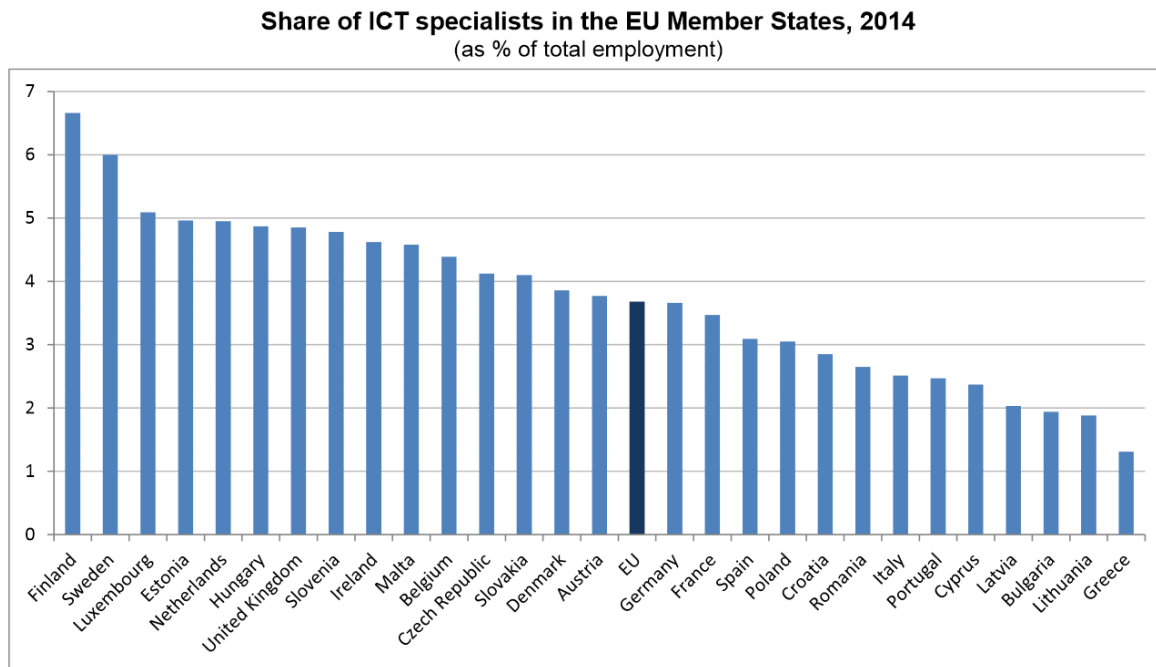
Um eine dynamische Szene rund um Universitäten, Startups und KMU's zu schaffen müssen ideale Rahmenbedingungen geschaffen werden. Der Bereich des Risikokapitals, um die Gründung von Startups zu fördern, scheint in Österreich unterausgestattet zu sein. Crowdfunding könnte hier ein neuer Weg zu sein, um neuen Unternehmen auch Risikokapital zur Verfügung zu stellen. Gerade auch in Zeiten wie diesen könnte auch aufgrund des sehr niedrigen Zinsniveaus die Beteiligung an Unternehmen für die breite Masse attraktiver gemacht werden.

Startups sind oft auch ein Inkubator für neue Ideen. Man versucht neue Wege zu gehen, die oft auch in eine Sackgasse führen. Manche davon funktionieren. Um das Risiko zu minimieren, rasch neue Dinge mit wenig Kapitalaufwand auszuprobieren, und falls es nicht funktioniert, sich auch wieder rasch Neuem zuwenden. Man spricht hier auch von „Fail Fast“. Es muss klar sein, dass Unternehmertum auch Risiko bedeutet und auch Investitionen in solche Unternehmen mit Risiko behaftet sind.

4.4.13 Forschung und Förderung

Die IKT Branche ist sehr forschungs- und entwicklungsintensiv und sie hat eine besonders große Hebelwirkung (Leverage-Effekt). Besonders die IKT Branche treibt den Fortschritt in der Digitalisierung voran. Leider haben wir gerade in Europa viele vor allem große Konzerne, die in diesem Bereich tätig waren, verloren (Siemens, Phillips, Olivetti, ...). Der Staat und Europa müssen gemeinsam überlegen, wie sie gerade für die Technologiebranche wieder attraktiver werden können.

Bei den IT Spezialisten liegt Österreich laut einer Eurostat Studie für 2014 gerade einmal im Mittelfeld:



Die Führenden Nationen in der EU sind Finnland und Schweden, die beinahe doppelt so viele IT Spezialisten haben, wie wir in Österreich.

Gerade die Förderung von Forschung und Entwicklung für den IKT Bereich könnte hier entscheidende Veränderungen herbeiführen. Im Schnitt werden einem geförderten Forschungsmitarbeiter in einem Unternehmen vier weitere zur Seite gestellt um die Forschungsergebnisse voran zu treiben. Investition in Forschung vor allem im IKT Sektor ist daher besonders sinnvoll. Hier wird aber auch allzu oft kritisiert, dass der Förderdschungel oft nicht zu durchblicken ist, und vermeintlich die Fördergelder nicht in die richtigen Projekte fließen.

Wir müssen jedoch auch dafür Sorge tragen, dass die notwendigen Spezialisten auch vom Bildungssystem zur Verfügung gestellt werden.

4.4.2 Bildung

4.4.2.1 Herausforderungen an das Bildungssystem

Die Digitalisierung hat erhebliche Auswirkungen auf die Bildung. Nicht nur, weil die Digitalisierung eine Auswirkung auf das Ausbildungssystem hat, sondern weil auch die Wirtschaft andere Arbeitskräfte benötigt, als die, die vom derzeitigen Bildungssystem "produziert" werden.

in 2020

1. Complex Problem Solving
2. Critical Thinking
3. Creativity
4. People Management
5. Coordinating with Others
6. Emotional Intelligence
7. Judgment and Decision Making
8. Service Orientation
9. Negotiation
10. Cognitive Flexibility

in 2015

1. Complex Problem Solving
2. Coordinating with Others
3. People Management
4. Critical Thinking
5. Negotiation
6. Quality Control
7. Service Orientation
8. Judgment and Decision Making
9. Active Listening
10. Creativity



Source: Future of Jobs Report, World Economic Forum

4.4.2.2 Digitale Alphabetisierung

Die „International Computer and Information Literacy Study“ erfasst die Medienkompetenzen von Schülern in der 8. Schulstufe im internationalen Vergleich. Folgende Kompetenzen werden dabei getestet:

- Kompetenzen zur Nutzung von Technologien zur Recherche von Informationen (z. B. im Internet)
- Die Fähigkeit, die gefunden Informationen im Hinblick auf ihre Qualität/Nützlichkeit zu bewerten

- Die Kompetenz, durch die Nutzung von Technologien Informationen zu verarbeiten und zu erzeugen
- Die Kompetenz, neue Technologien zur Kommunikation von Informationen zu nutzen
- Kompetenzen für einen verantwortungsvollen und reflektierten Umgang mit IKT.

Es zeigt sich bei diesem Test, dass die „digital Natives“ zwar mit Computern umgehen können, aber in weiten Bereichen mit dem Einsatz, den Vorteilen und den Problemen des Einsatzes nicht so vertraut sind wie man vermuten möchte. Hier muss also gerade im Bereich der Vermittlung von Medienkompetenz angesetzt werden.

Besonders wichtig in diesem Zusammenhang ist nicht nur die Vermittlung von Wissen über die Anwendung der Technologie, sondern auch Wissen über die gesellschaftlichen Auswirkungen, wie rechtliche Rahmenbedingungen (Urheberrecht). Oft ist jungen Menschen gar nicht bewusst, welchen Gefahren sie durch Umgang mit digitalen Medien ausgesetzt sind. (Beispiel: Postings von privaten Fotos auf Facebook bzw. SnapChat, Nutzung der Daten durch Online Anbieter, etc.).

4.4.2.3 Ausstattung

Die Digital Society hat an der Erstellung des vor kurzem vorgelegten "Grünbuch Digitaler Wandel" mitgearbeitet. Dort wurde angeregt, alle Schulklassen mit Tablets und alle Schüler mit E-Mail-Adressen auszustatten. Die Idee ist prinzipiell gut, greift aber erheblich zu kurz.

Einer unserer Mitgliedsvereine (ClubComputer – damals noch als Personal Computer Club am TGM, kurz PCC-TGM) hat sich bereits 1986 darum bemüht, HTL Schülern eine adäquate Ausstattung zu bieten und Schulen mit PCs auszustatten. Heutzutage sind wohl die meisten Schülerinnen und Schüler mit Computer, Laptop oder Tablet ausgestattet, jedoch stellt eine solche Anschaffung weiterhin für Familien eine finanzielle Belastung dar. Diese digitale Kluft gilt es zu schließen.

Zu bedenken ist, dass Computer, Laptops und Tablets nur Werkzeuge sind und noch nicht die Lösung. Die technische Entwicklung findet so rasant statt, dass Lehrinhalte kaum mehr Schritt halten können. Eine Bring Your Own Device (BYOD) Strategie (ggf. mit staatlicher Förderung) ist hier sicherlich zielführender als Leih-Tablets, oder Notebook Klassen.

Eine große Menge an Lehrinhalten wird nur „analog“ zur Verfügung gestellt. Es werden jährlich ca. 100 Mio. EUR aus dem FLAF (Familienlastenausgleichsfonds) in die Schulbuchaktion investiert. Würden Teile dieses Budgets dazu verwendet, freie (im Sinne des Urheberrechts – „OER“ Open Educational Resources) digitale Lernhilfen bereitzustellen, die auch laufend aktualisiert werden können, könnte auch in diesem Bereich ein großer Schritt vorwärts gemacht werden. Gerade das Urheberrecht ist im Bereich der Ausbildung sehr oft ein massiver Klotz am Bein.

4.4.2.4 Nutzung

Die Arten der Nutzung digitaler Technologien unterliegen einem dauernden Wandel. Ist die Verwendung von E-Mail noch gut, um sich für Online-Dienste wie Facebook oder WhatsApp zu registrieren – für persönliche Kommunikation wird dieser Dienst so gut wie gar nicht mehr genutzt.

Auf diese Veränderungen muss auch im Ausbildungssystem Rücksicht genommen werden. Schülerinnen und Schülern muss eine moderne Infrastruktur für kollaboratives Arbeiten und Lernen in der Schule zur Verfügung gestellt werden.

Hier existieren innovative Ideen. Gamification⁹ erweist sich als überragende Methode, die mühsamen, teilweise sehr administrativen Tätigkeiten im Schulalltag aufzulockern und Jugendliche wie Lehrende zu motivieren. [Classcraft](#)¹⁰ setzt beispielsweise auf Rollenspielelemente, um Motivation und damit Konzentration zu erhöhen, Teamfähigkeiten zu fördern und Spannungen abzubauen.

4.4.2.5 Ort und Zeit

Ähnlich wie die Arbeitswelt unterliegt auch die Ausbildung einer Dezentralisierung. Man muss heute nicht mehr physisch an einen Ort gehen, um zu lernen. Digitale Dokumente und Videostreams bringen hochqualitative Lehrinhalte und Lehrende aus aller Welt zu jedem denkbaren Thema in jedes Klassenzimmer, aber auch in alle anderen Räumlichkeiten und schaffen die Möglichkeit, Schülerinnen und Schüler von überall her am Unterricht teilnehmen zu lassen.

⁹ Als Gamification (von englisch „game“ für „Spiel“) bezeichnet man die Anwendung spieltypischer Elemente und Prozesse in spielfremdem Kontext. (aus Wikipedia)

¹⁰ <http://www.classcraft.com/de/>

Das physische Beisammensein bleibt wichtig und notwendig, um soziale Kontakte und Teamfähigkeit aufzubauen, nicht aber für den Unterricht, den Transport von Wissen per se.

Unter diesen Aspekten ist zu überlegen, ob Schulgebäude diese Ansprüche überhaupt noch optimal unterstützen.

4.4.2.6 Unser Schulsystem

Wir haben gerade eine "große" Bildungsreform hinter uns (und deren Umsetzung vor uns).

Unser Schulsystem – so wie wir es kennen – stammt aus dem 19. Jahrhundert und wurde als dreistufiges Ausbildungssystem eingerichtet, das bis heute erhalten ist:

1. Die Pflichtschuljahre (Volksschule und Unterstufe)
hatten zum Ziel, Fabrikarbeiter heranzuziehen. Am Beginn der Industrialisierung wurden Arbeiter benötigt, die repetitive Tätigkeiten ausführen ohne über deren Sinnhaftigkeit allzu sehr nachzudenken. "Einheitsmenschen", die gut ersetzbar waren.
2. Die Oberstufenjahre
hatten zum Ziel, Verwaltungsbedienstete (von denen es wenige gab) für diese Fabriken und den Staat auszubilden.
3. Das Universitätsstudium
hatte zum Ziel, Menschen für Wissensberufe wie Ärzte, Rechtsanwälte, oder Lehrer heranzuziehen. Davon gab es noch viel weniger als Verwaltungsbedienstete.

Heutzutage sehen die Anforderungen an die Kenntnisse und Eigenschaften von Mitarbeiter in der digitalen Welt so aus:

- kreativ
- teamfähig
- eigenverantwortlich
- vernetzt

Der US Wissenschaftler George Land untersuchte in einer Studie Ende des 20. Jahrhunderts¹¹, welche Auswirkungen die "moderne" Schulausbildung auf die Fähigkeiten unserer Jugend hat. Er testete die Kreativität von 1600 Kinder ab dem Alter von 5 Jahren mit einem für die NASA entwickelten Test, mit dem diese die Kreativität von Astronautenanwärtern misst. Diesen Test wiederholte er bis ins Erwachsenenalter. Die Ergebnisse stimmen nachdenklich. Für den Anteil an hochgradig Kreativen in den jeweiligen Altersstufen fand man:

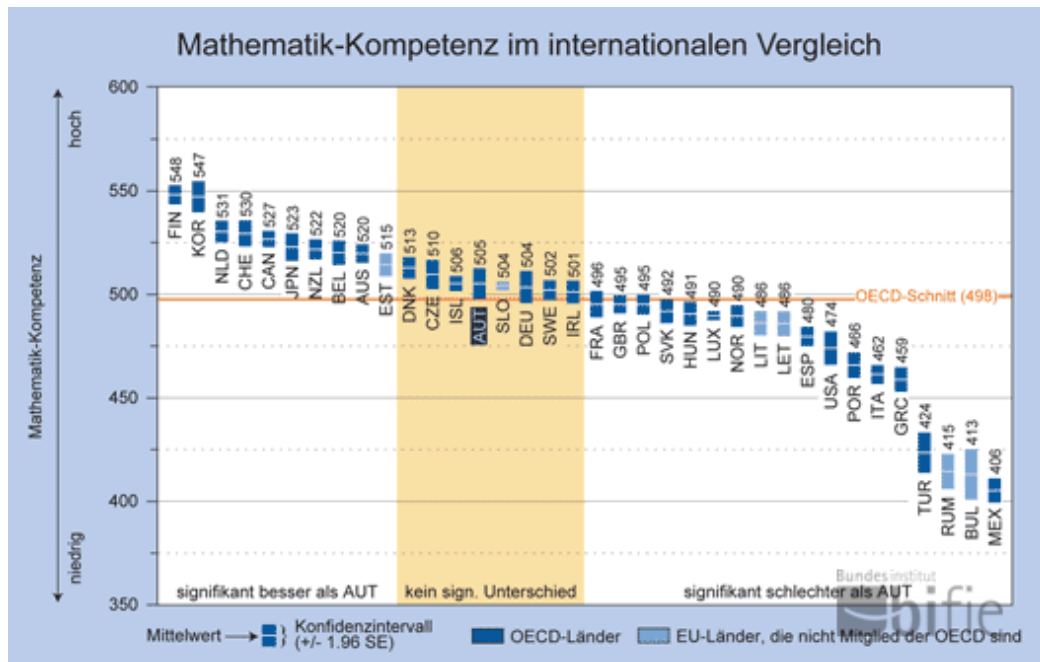
- 5-jährige: 98%
- 10-jährige: 30%
- 15-jährige: 12%
- Erwachsene: 2%

Unser Bildungssystem leistet also hervorragende Arbeit. Es macht uns zu braven Fabrikarbeitern, die ihre Aufgaben durchführen, ohne hochgradig kreativ und vernetzt zu denken. Das entspricht zwar den Anforderungen von um 1900, aber nicht den oben genannten, von den Unternehmen gewünschten Fähigkeiten.

Unser Bildungssystem wird laufend weiterentwickelt, neue Lehrmethoden versuchen die obigen Fähigkeiten zu stärken, basiert aber noch immer auf dem starren 3-Stufen-System. Wird unsere soeben mühsam auf den Weg geschickte "große Bildungsreform" diese Probleme angehen und lösen? Eher nicht. Die Probleme liegen bedeutend tiefer.

Im internationalen Vergleich liegt Österreich im Mittelfeld (OECD Schnitt). Das zeigt auch die PISA Studie:

¹¹ <http://www.creativityatwork.com/2012/03/23/can-creativity-be-taught/>



4.4.2.7 Erwachsenenbildung

Ein wichtiger Punkt ist auch, die Bildung von älteren Personen nicht zu vergessen. Vor allem diese Personen haben oft Probleme, den Anschluss nicht zu verlieren, sind skeptisch gegenüber neuen Technologien und werden durch die voranschreitende Digitalisierung in manchen Bereichen an den Rand der Gesellschaft gedrängt. Es ist hier wichtig, diesen Personen den Zugang zu diesen Technologien zu ermöglichen und entsprechendes Wissen zu vermitteln und die Scheu davor zu nehmen. Eine entsprechende Förderung dieser Aktivitäten durch Staat und/oder Industrie wäre wünschenswert. Hier leistet auch unser Mitglied ClubComputer einen Beitrag.

5 Grundrechte

Grundrechte sind wesentliche Rechte, die Mitgliedern der Gesellschaft gegenüber Staaten als beständig, dauerhaft und einklagbar garantiert werden. In erster Linie sind sie Abwehrrechte des Bürgers gegen den Staat.

Leider werden Grundrechte in der "digitalen Welt" oft nicht mehr so ernst genommen wie in der analogen. Würde der Staat Zensoren in ein Postamt setzen, die alle Briefe aufreißt und mitlesen, dann hätten wir sofort Demonstrationen. Wenn der Staat das gleiche digital macht, nämlich den gesamten Datenverkehr mitliest, dann wird das mit einem Achselzucken beantwortet.

5.1 Welche Grundrechte gibt es?

Grundrechte sind Rechte, die für unsere gesamte Gesellschaft und das Funktionieren unseres demokratischen Rechtsstaates von entscheidender Bedeutung sind. Wichtige Grundrechte sind:

- Recht auf Freiheit, Eigentum und Sicherheit der Person
- Allgemeine, nur durch Gesetz beschränkbare Handlungsfreiheit
- Freiheit von willkürlichen Eingriffen in die Privatsphäre etc.
- Meinungsfreiheit
- Gedanken-, Gewissens- und Religionsfreiheit
- Reisefreiheit
- Versammlungs- und Demonstrationsfreiheit
- Informationsfreiheit
- Berufsfreiheit

Aufgrund spätestens der Enthüllungen von Edward Snowden wurde deutlich, dass sich z.B. die NSA nicht an die US Verfassung hielt und sogar den Kongress wissentlich belogen hat.

Man stelle sich einmal vor, dass ein staatlicher Kommissär in jedem Postamt sitzen würde, dort alle Briefe aufreißen und dem Staat darüber Bericht erstatten würde. Genau das ist durch die vollständige Überwachung der elektronischen Kommunikation zumindest durch Geheimdienste wie NSA und GCHQ in UK heute aber Realität. Unsere digitale Kommunikation ist vor Übergriffen des Staates überhaupt nicht mehr geschützt.

Man stelle sich auch vor, dass jeder Bürger einen Polizisten beiseite gestellt bekommt, der ihn auf Schritt und Tritt überwacht, alle seine Bewegungen aufzeichnet und diese Aufzeichnungen dann zentral für viele Jahre gespeichert werden – auf die im Bedarfsfall zugegriffen werden kann. Genau das hat die Vorratsdatenspeicherung versucht.

Den Vogel abgeschossen hat die britische Regierung, als sie Alan Rusbridger eingeschüchtert und zur Herausgabe der Daten von Edward Snowden gezwungen hatte, und das übergebene Notebook dann mit einem Vorschlaghammer zerstört hat. Soviel zum Thema Pressefreiheit in Europa. Es war ziemlich klar, dass die Regierung hier nicht zufrieden war, was die Medien hier publizierten und ein Zeichen setzen wollte – als Warnung für andere Medien.

Wir reden immer darüber, dass wir unsere westlichen Werte verteidigen müssen. Man muss sich aber bewusst werden, dass wir – wenn wir diese Rechte einschränken – auch unsere Freiheit und unsere Demokratie insgesamt einschränken.

Unser Ziel ist es, die Grundrechte – wie sie aus der “analogen” Welt vollkommen selbstverständlich sind – auch in der digitalen Welt in Erinnerung zu rufen und wiederherzustellen.

5.2 Meinungsfreiheit

Durch die Digitalisierung ist auch die Meinungsfreiheit in Gefahr. Bei Demonstrationen ist es für die Polizei möglich durch IMSI Catcher eine fast vollständige Teilnehmerliste zu erstellen. Ebenso ermöglicht Gesichtserkennungssoftware Teilnehmer zu identifizieren und Listen von „verdächtigen Personen“ zu erstellen.

Die spätestens seit Edward Snowden bekannte Totalüberwachung des Internets bringt für die Sicherheitsbehörden weitere Möglichkeiten unliebsame „Störenfriede“ zu überwachen. Dabei ist ein Störenfried nur jemand der sich den Verdacht von Sicherheitsbehörden zuzieht – aber nicht jemand der von einem ordentlichen Gericht als einer identifiziert wird. Und genau hier liegt das Problem.

Die derzeit in Europa eingeführte und mit den USA schon existente Fluggastdatenspeicherung liefert eine weitere Möglichkeit die Bürger zu überwachen.

Man muss also nicht einmal etwas anstellen um ins Raster der Gesetzeshüter zu gelangen – und es sind ausreichend Beispiele (auch in der „freien Welt“ bekannt) in dem die „Gesetzeshüter“ gegen unliebsame Bürger vorgegangen sind, obwohl diese nie gegen Gesetze verstoßen hatten. In Österreich wäre an dieser Stelle der „Tierschützerprozess“ zu nennen. In UK die Vernichtung der Snowden Festplatten. Dies diene alles dazu, unliebsame Personen dazu zu bringen von ihrer Meinung abzulassen und zum Schweigen zu bringen.

Ein weiterer Fall der Einschränkung der Meinungs- und Redefreiheit sind die willkürlichen Zensurmaßnahmen von Facebook. Inhalte die nicht den Benützungsbedingungen entsprechen werden gelöscht. So gibt es die skurrilen Situationen, dass Facebook Fotos von nackten Frauenbrüsten zensuriert, Neonazipropaganda und Filme von Hinrichtungen aber nicht gegen die Nutzungsbedingungen von Facebook verstoßen. Der dänische Autor Peter Ovig führte z.B. mit den Fans seines Buches einen Kampf gegen die Zensur von Facebook, die künstlerische Bilder, die auf Facebook gepostet wurden, tausendfach zensurierte, weil auf den Bildern nackte Frauenbrüste abgebildet waren. Facebook setzt dazu s.g. „Content Moderators“ ein, also Moderatoren – oder besser gesagt Zensoren. Diese Zensoren zensurieren nach den Benutzungsbedingungen mit Facebook – nicht nach Gesetzen – und schon gar nicht erst nach einer richterlichen Anordnung. Willkür ist hier also Tür und Tor geöffnet.

5.3 Brief- Kommunikationsgeheimnis

In der analogen Welt ist es möglich Briefe zugeklebt zu verschicken. Diese Möglichkeit ist uns im Internet abhandengekommen, da staatliche Institutionen immer und überall mithören können. Daraus lässt sich ableiten, dass Kommunikation im Internet nur noch verschlüsselt übertragen werden darf um das entsprechende Grundrecht wiederherzustellen.

Die Möglichkeit diese Kommunikation abzuhören muss daher technologisch schwieriger gemacht werden.

Wir sind uns im Klaren, dass jegliche Verschlüsselung auch gebrochen werden kann. Jedoch sollte das nur mit erheblichem Aufwand möglich und nur nach richterlichem Befehl durchgeführt werden dürfen. Genauso wie ein Haus nur nach einer richterlichen Anordnung durchsucht werden darf. Das Verbot von Verschlüsselungstechnologien wäre gleichzusetzen mit dem Verbot von Schlössern auf Türen, damit die Polizei jederzeit ein Haus betreten kann. Das hieße aber auch, dass jedermann jederzeit ins Haus könnte.

Der Ruf nach „Hintertüren“ (Back Doors) durch die Geheimdienste ist gefährlich. Denn solche Back Doors werden sicher nicht nur durch Geheimdienste genutzt, sondern auch von denjenigen vor denen wir uns schützen wollen.

5.3.1 Vorratsdatenspeicherung

Unter Vorratsdatenspeicherung versteht man die Speicherung personenbezogener Daten durch oder für öffentliche Stellen, ohne dass die Daten aktuell benötigt werden. Sie werden also nur für den Fall gespeichert, dass sie einmal benötigt werden sollten. In der rechtspolitischen Debatte bezieht sich der Begriff meist auf die Vorratsdatenspeicherung von Telekommunikations-Verbindungsdaten. (Telefongespräche, E-Mails, etc.).

Diese betrifft die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Registrierung der Verbindungsdaten elektronischer Kommunikationsvorgänge (sogenannte Metadaten, ohne dass ein Anfangsverdacht oder eine konkrete Gefahr besteht (Speicherung bestimmter Daten auf Vorrat). Erklärter Zweck der Vorratsdatenspeicherung ist die verbesserte Möglichkeit der Verhütung und Verfolgung schwerer Straftaten.

In Österreich wurde die Vorratsdatenspeicherung am 1. April 2012 durch eine Novelle des Telekommunikationsgesetzes (TKG) 2003 eingeführt.

In Österreich hatten die Kärntner Landesregierung, ein Angestellter eines Telekommunikationsunternehmens, sowie über 11.000 Privatpersonen (darunter auch einige unserer Mitglieder) organisiert durch die AK Vorrat gegen das Gesetz geklagt. Der Verfassungsgerichtshof brachte die Sache vor den EuGH um zu klären ob die anlasslose Massenüberwachung mit den EU Grundrechten vereinbar wären. Dieser erklärte daraufhin die EU Richtlinie zur Vorratsdatenspeicherung am 8.4.2014 für ungültig und hob diese auf.

Nachdem der EuGH die Richtlinie aufgehoben hatte, erklärte der Österreichische Verfassungsgerichtshof die Vorratsdatenspeicherung für unzulässig. Der Verfassungsgerichtshof begründete seine Entscheidung G 47/2012 damit, dass ein so gravierender Grundrechtseingriff so gestaltet sein muss, dass er mit dem Datenschutzgesetz und der Europäischen Menschenrechtskonvention im Einklang steht

Da es die Vorratsdatenspeicherung in Österreich fast zwei Jahre lang gab, wurden auch Erfahrungen darüber gesammelt, welche Erfolge die Sicherheitsbehörden durch den Zugriff auf die Vorratsdaten vorweisen konnten. In keinem einzigen Fall wurde sie zur Bekämpfung von Terror angewendet¹².

5.4 Fluggastdaten / Passenger Name Record (PNR)

5.4.1 Was sind Fluggastdaten / Passenger Name Record (PNR)



Welche Daten umfasst ein Passenger Name Record (PNR)? Die Fluglinien müssten natürlich, um den Flugbetrieb aufrecht zu erhalten, Daten über Ihre Passagiere speichern. Diese Passagierdaten umfassen nicht nur Namen und die Flugdaten selbst sowie Sitzplatz des Passagiers, sondern auch eine Reihe zusätzlicher Informationen:

1. PNR (Passenger Name Record)-Buchungscode (Record Locator)
2. Daten der Reservierung / der Ausstellung des Flugscheins
3. Geplante Abflugdaten
4. Name(n)
5. Verfügbare Vielflieger- und Bonusdaten (das heißt Gratisflugscheine, Upgrades, usw.)
6. Andere Namen im PNR einschließlich Zahl der Reisenden im PNR
7. Alle verfügbaren Kontaktinformationen (einschließlich Angaben zum Buchenden)
8. Alle verfügbaren Zahlungs-/ Abrechnungsinformationen (ohne weitere Transaktionsdetails für eine Kreditkarte oder ein Konto, die nicht mit der die Reise betreffenden Transaktionen verknüpft sind)
9. Reiseverlauf für den jeweiligen PNR
10. Reisebüro/ Sachbearbeiter
11. Code-Sharing-Informationen
12. Informationen über die Aufspaltung/ Teilung einer Buchung
13. Reisestatus des Passagiers (einschließlich Bestätigungen und Eincheckstatus)
14. Informationen über Flugscheinausstellung (Ticketing) einschließlich Flugscheinnummer, Angabe, ob Flugscheine für einfachen Flug (One-Way) sowie Automatic Ticket Fare Quote (automatische Tarifabfrage)

¹² https://www.parlament.gv.at/PAKT/VHG/XXIV/AB/AB_14397/imfname_314525.pdf

- 15. Sämtliche Informationen zum Gepäck
- 16. Sitzplatzinformationen einschließlich der Sitzplatznummer
- 17. Allgemeine Bemerkungen einschließlich OSI, SSI und SSR
- 18. Etwaig erfasste APIS¹³-Daten
- 19. Historie aller Änderungen der unter den Nummern 1 bis 18 aufgeführten PNR

5.4.2 Fluggastdatenaustausch EU / USA

Das Europaparlament hat im April 2012 dem sehr umstrittenen Fluggastdatenabkommen (Passenger Name Record – PNR) zugestimmt – nachdem die USA massiven Druck auf Europa ausgeübt hat. Die Daten werden schon seit 9/11 an die USA weitergegeben – jedoch ohne rechtliche Grundlage. Dieses Abkommen dient zur Legalisierung dieser Datenweitergabe – und vor allem dem Schutz der Fluglinien, wegen Verstoßes gegen Datenschutzgesetze.

5.4.2.1 Wer ist davon betroffen?

Betroffen ist davon jeder Bürger, der aus der Europäischen Union in die USA einreist.

5.4.2.2 Wer ist der Empfänger der Daten

Die Daten werden an das Department of Homeland Security (Heimatschutzministerium) übermittelt. Das ist das mächtige Grenzschutzministerium der USA, in das das ehemalige Department of Border Protection integriert wurde.

5.4.2.3 An wen werden die Daten noch übermittelt

Das DHS (Department of Homeland Security) darf und wird die Daten auch an andere US Behörden weiterleiten, darunter auch den CIA (Auslandsgeheimdienst), die NSA, etc. Auch dürfen die US Behörden die Daten auch an Drittstaaten weitergeben. Die betroffenen Personen haben also keine Ahnung wo ihre Daten letztendlich landen, und wer auf diese Daten Zugriff hat.

¹³ APIS – Advance Passenger Information Service

5.4.2.4 Wie lange bleiben die Daten gespeichert?

Die Daten bleiben **15 Jahre** gespeichert. Danach werden sie irreversibel anonymisiert, aber nicht gelöscht. Die Daten bleiben die ersten 5 Jahre in einer aktiven Datenbank. Dabei werden nach 6 Monaten Name und Kontaktinformationen ausgeblendet. Danach werden die Daten (mit ausgeblendeten Namen und Kontaktinformationen) in eine ruhende Datenbank übergeführt. Über den gesamten Zeitraum von 15 Jahren können die Daten jederzeit von der Behörde wieder entanonymisiert werden (die „Anonymisierung“ durch Ausblenden des Namens ist also keine wirkungsvolle Maßnahme zum Schutz der Privatsphäre). Über den gesamten Zeitraum können auch Rasterfahndungen mit den Daten durchgeführt werden, bzw. die Daten auch mit anderen Datenbanken abgeglichen werden.

5.4.3 Innereuropäische Fluggastdatenspeicherung

Nach den [Terroranschlägen am 13. November 2015](#) in Paris haben sich die EU Innenminister darauf geeinigt die lange nicht durchsetzbare Fluggastdatenspeicherung nun auch in der EU umzusetzen. Ziel der Verordnung ist die Bekämpfung des Terrorismus.

5.4.3.1 Wer ist davon betroffen?

Passagiere die die EU verlassen oder in die EU einreisen verpflichtend. Innereuropäische Flüge können erfasst werden, müssen aber nicht. Die Entscheidung darüber obliegt den einzelnen Mitgliedsländern. Passagiere müssen von der Verarbeitung und Speicherung dieser Daten in geeigneter Form in Kenntnis gesetzt werden.

5.4.3.2 Wer ist der Empfänger der Daten?

Die Daten werden von den Fluglinien den Sicherheitsbehörden der einzelnen EU Mitgliedsländer übermittelt. Es ist eine Zentrale Verarbeitungsstelle einzurichten, die für die Verarbeitung der Daten zuständig ist.

5.4.3.3 Wie lange bleiben die Daten gespeichert?

Die Daten bleiben 30 Tage im Klartext gespeichert und danach 5 Jahre anonymisiert.



- Wir glauben, dass die Weitergabe der Fluggastdaten durch die Fluglinien an die USA der EU Grundrechtscharta widerspricht.
- Wir glaube auch, dass die Sammlung der PNR Daten von Reisenden in und aus der EU, sowie vor allem innerhalb der EU den EU Grundrechten widerspricht. Durch die Totalüberwachung des Flugverkehrs wird unzumutbar in die persönlichen Freiheiten eingegriffen. Eine Verhältnismäßigkeit ist wie schon zuvor bei der Vorratsdatenspeicherung nicht zu erkennen.
- **Sensible Daten:** Aus den Informationen sind auch z.B. Rückschlüsse über Religionsbekenntnisse (über Essenswünsche), Gesundheitszustände (angeforderter Rollstuhl, Essenswünsche), Fluggewohnheiten (Vielfliegerprogramm), sexuelle Orientierung (über Reisebegleiter und gemeinsame Buchungen), etc. ablesbar
- Eines der Grundprobleme von solchen verdachtsunabhängigen Datensammlungen ist, dass unbescholtene Bürger durch Zufälle in das Netz der Fahnder kommen können, was bei der derzeitigen Menschenrechtslage in den USA mehr als gefährlich ist. Man ist auch als EU Bürger nicht davor geschützt – ohne Angabe von Gründen von den Behörden bei der Einreise in den USA festgehalten zu werden.
- Die Digital Society könnte sich eine Speicherung dieser Daten nur in verschlüsselter Form vorstellen, Zugriff auf diese Daten sollte nur nach Richtervorbehalt in Einzelfällen möglich sein, wenn begründete Verdachtsmomente bestehen.
- Predictive Policing in jeglicher Art ist abzulehnen.

5.5 Staatsschutzgesetz

In Österreich soll Anfang 2016 ein neues Staatsschutzgesetz beschlossen werden. Das Staatsschutzgesetz überträgt dem BVT (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung) – eigentlich eine Polizeibehörde - die Befugnisse eines Geheimdienstes.

Der Hauptkritikpunkt ist, dass das BVT im Grunde jeden überwachen darf. Ohne Richter und konkreten Tatverdacht.

Das BVT kann auf Daten aller Behörden und aller Firmen zugreifen, ohne Richter.

Lediglich der Rechtsschutzbeauftragte des BM.I. und seine Stellvertreter überwachen derartige Zugriffe. (Die Behörde überwacht sich also selbst). Das BVT kann jedoch den Datenschutzbeauftragten die Akteneinsicht verwehren um Zeugen zu schützen.

Die Aufgabe des BVT ist der Schutz der Staatlichen Institutionen. Aus diesem Grund kamen auch schon in der Vergangenheit meist nicht Terroristen, sondern andere „Störenfriede“ ins Visier des BVT – wie z.B. [Tierschützer](#)¹⁴ oder Demonstranten die z.B. gegen den Akademikerball demonstriert hatten.

Das BVT speichert die Daten über Personen die ins Visier des BVT kommen 6 Jahre lang. Zugriffsprotokolle auf diese Daten werden nur 3 Jahre lang aufgehoben. **Das BVT darf alle Daten auch mit ausländischen Geheimdiensten austauschen.** Daher sind die Behaltefristen und jeglicher Schutz der Daten hinfällig.



- Polizeibehörden benötigen einen Verdachsmoment und um in die Privatsphäre von Menschen einzudringen eine richterliche Anordnung. So ist es unmöglich, dass sich eine Polizeibehörde selbstständig macht.
- Eine Behörde mit derart umfangreichen Befugnissen benötigt auch eine adäquate Kontrolle durch Richter und Parlament
- Die Übermittlung der Daten an ausländische Geheimdienste ohne jegliche Kontrolle zu erlauben ist grob fahrlässig.

14

https://de.wikipedia.org/wiki/Wiener_Neust%C3%A4dter_Tiersch%C3%BCtzerprozess#Kritik_an_den_Ermittlungsbeh.C3.B6rden

6 Urheberrecht & digitale Medien



Urheberrecht und digitale Medien sind eng miteinander verknüpft. Sobald Medien in digitaler Form vorliegen ist es sehr einfach sie zu vervielfältigen. Das verändert die notwendigen Geschäftsmodelle grundlegend für Musik, Film, Foto, Bücher, ...

Die Broschüre [Medien in Österreich](#)¹⁵ des Bundeskanzleramtes gibt einen Überblick

über die Medienlandschaft in Österreich.

6.1 Faire Entlohnung für künstlerische Arbeit

Künstler zu sein ist nicht unbedingt ein leichter Beruf. Wir wollen, wenn wir am Abend heimkommen, einen Film im Fernsehen ansehen und dabei entspannen – oder am Wochenende ins Kino gehen. Wir nutzen die Zeit, die wir im Auto verbringen, um Radio oder MP3 zu hören, oder freuen uns darauf ein gutes Buch zu lesen. Das alles ist nur möglich, weil es Künstler gibt, die gute Musik produzieren; gute Schauspieler, die in Filmen mitspielen; Autoren, die Bücher schreiben; oder Maler oder auch Fotografen, die tolle Bilder machen. Wir verstehen daher, dass Künstler für Ihre Arbeit auch einen fairen Lohn erhalten wollen – wie wir anderen, die diese Werke dann auch genießen.



- Das Publikum / die Konsumenten haben Interesse an Kunst. Künstler und Publikum haben daher ein gemeinsames Interesse daran dass es Künstler gibt, und diese wird es nur geben, wenn es auch möglich ist vom Beruf des Autors, Musikers oder Schauspielers zu leben.

¹⁵ <https://www.bka.gv.at/DocView.axd?CobId=57669>

6.2 Privatkopie und Publikum

Was wir als Anwender allerdings nicht verstehen, ist, dass man uns in letzter Zeit immer wieder versucht in ein kriminelles Eck zu drängen. Jeder Nutzer ist ein "Raub"-Kopierer. Schon alleine dieses Wort ist falsch – ich habe noch nie einen "Raub"-Kopierer gesehen, der einen Künstler mit einer Waffe bedroht und ihm gewaltsam sein Werk entwendet hätte (das ist es, was Raub bedeutet). Viele Konsumenten, die immer legal Musik und Filme erworben haben, kommen sich ziemlich dumm vor, weil einem immer vorgehalten wird, dass ohnehin alles illegal aus dem Internet gesaugt wird. Manche Konsumenten empfinden die diversesten Kampagnen schon als "Publikumsbeschimpfung" und das ist nicht unbedingt zielführend – denn die Künstler brauchen auch uns Anwender, nämlich auch als ihr Publikum.



- Die Urheberrechtsabgabe entstand aus dem Wunsch die Kriminalisierung durch die Privatkopie zu beenden. Schüler sollten nicht mehr verfolgt werden können, wenn sie die Hitparade selbst von Ö3 auf Radiokassetten aufnehmen.
- Durch die neue Urheberrechtsreform ist das leider aber wieder geschehen. Privatkopien aus nicht legalen Quellen (was ist das eigentlich genau) sind wieder illegal. MP3 Tauschen am Schulhof (meist durch P2P Werkzeuge) ist daher wieder illegal.
- Die neue Speichermedienabgabe (aka Festplattenabgabe) hat die Einnahmen von 16Mio in Spitzenzeiten nun auf 30 Mio fast verdoppelt. Das Rechte auf Privatkopie wurde aber defakto abgeschafft.

6.3 Überwachung

Vor allem aus den USA wird die Forderung laut, das Urheberrecht mit eiserner Faust durchzusetzen. Internet Provider sollen Hilfssheriffs spielen, die Kommunikation ihrer Kunden überwachen und diese bei illegalen Aktivitäten dann "vernadern" müssen. Dieser Eingriff in die Grundrechte ist gravierend und daher vollständig abzulehnen.



- Die Frage, ob das Recht auf Privatsphäre oder das Copyright höher zu bewerten sei, ist in Europa bisher immer zu Gunsten der Privatsphäre beantwortet worden.
- Eine Totalüberwachung des Internet zur Durchsetzung es Copyrights ist abzulehnen.

6.3.1 Nachteile für ehrliche Käufer

Zudem hat man als Käufer oft Nachteile. Kopierschutz oder Verschlüsselungstechnologien machen dem Käufer das Leben schwer (Blu-ray kann z.B. nicht auf VGA Bildschirmen wiedergegeben werden), ein minutenlanger Vorspann erklärt dem Käufer, dass Raubkopieren böse ist – ein Raubkopierer sieht diesen Vorspann natürlich nicht mehr, denn er wurde schon lange Zeit vorher entfernt.

Bei Streaming Diensten hat man das Risiko – dass es den Dienst eventuell irgendwann nicht mehr gibt, und man auf die Daten nicht mehr zugreifen kann (was wäre z.B., wenn Amazon nicht mehr existieren würde, mit den Kindle Büchern?). Microsoft hat unlängst seinen Zune Dienst eingestellt. Da der Zune Player offiziell nie in Europa verfügbar war, hat das hierzulande kaum eine Auswirkung, aber generell zeigt es das Problem auf.

Bei iTunes bezahlt man beim Erwerb des Musikstücks auch bereits die Privatkopie. Man darf die erworbenen Musikstücke bereits durch den Erwerb auf all seinen Geräten benutzen und abspielen. Durch die Speichermedienabgabe hat der Konsument das Gefühl doppelt abkassiert zu werden.

Auch Gebietsschutz – vor allem innerhalb der EU, aber auch außerhalb limitiert den Nutzer. Warum kann sich z.B. ein Konsument einen Bericht des ZDF ansehen, nicht aber über das Internet auf die TvThek der ARD zugreifen?



- Käufer sollten für den Kauf von Medien belohnt und nicht bestraft werden. Unsinnige Ermahnungen und Sicherungsmaßnahmen die ohnehin jeder Volksschüler umgehen kann tragen nicht dazu bei, dass Kunden nach einem Kauf zufrieden sind.

6.4 Veränderungen in der Medienlandschaft

Durch die "Revolution" am Mediensektor – Medien werden nicht mehr physisch produziert (Schallplatten, CD's, DVD's, Bücher), hier spart man an Produktionskosten, es wird eine Menge an Logistik eingespart – muss man nicht mehr mit LKWs die Medien transportieren, gibt es keine Notwendigkeit für riesige Lager und auch große teure Geschäfte / Verkaufsflächen. Daher gibt es für viele Künstler auch nicht mehr wirklich die Notwendigkeit Leib und Seele an große Medienkonzerne zu verkaufen. Die Medienkonzerne (sogenannte Rechteinhaber) haben lange Zeit genau diese Aufgabe übernommen. Sie haben Medien produziert, für die Verteilung und Vertrieb gesorgt. Diese Rolle übernehmen nun andere Firmen – wie z.B. Amazon.com (für Bücher) oder Apple (für Musik). Die großen Medienkonzerne – die die Zeichen der Zeit verschlafen haben – versuchen nun mit allen ihnen zur Verfügung stehenden Mitteln, alte und obsolete Geschäftsmodelle zu behüten. Über Lobbying bei Gesetzgebern versucht man daher eine Verschärfung des Urheberrechts durchzusetzen. Man versucht Internet Provider dazu zu zwingen, ihre eigenen Kunden auszuspionieren und zu überwachen. Es gibt auch vielfach Versuche, das in Österreich herrschende Recht auf Privatkopie abzuschaffen und Urheberrechtsverletzungen als strafrechtliche Delikte (derzeit sind es privatrechtliche Delikte) zu verankern. Das Urheberrecht darf nicht dazu dienen überholte Geschäftsmodelle zu retten.



- Attraktive Geschäftsmodelle sind der Schlüssel für Profite mit Medien. Aktuelle Entwicklungen müssen von den Konzernen aufgeschlossen aufgenommen werden.
- Der Versuch Geschäftsmodelle die vorgestern funktioniert haben ins nächste Jahrhundert durch die Verschärfung von Gesetzen zu retten, wird scheitern.

6.5 Festplattenabgabe / Speichermedienabgabe

Da sind dann noch die Verwertungsgesellschaften. Da in Österreich und anderen Staaten im Urheberrecht das Recht auf Privatkopie verankert ist, wurden die Verwertungsgesellschaften wie Literar-Mechana, Austro Mechana, AKM, VG-Rundfunk, etc. per Gesetz ermächtigt, selbst Steuern einzuheben – und zwar auf Leermedien. Da früher fast ausschließlich Kassetten als Leermedien eingesetzt wurden – nennt sich diese Abgabe auch Leerkassettenvergütung. Diese Leerkassettenvergütung ersetzt den Verdienstentgang der Künstler, der durch das private Kopieren von Werken (z.B. Aufnahme aus dem Fernsehen oder Radio oder Kopie von Medien) entsteht. Da in der heutigen Zeit immer weniger Leermedien zur Anwendung kommen, versucht man den Entgang der Einnahmen durch kreative Steuern auf andere Datenspeicher zu kompensieren. Mittlerweile werden Abgaben auf Festplatten, Speicherkarten, USB-Sticks und auch auf ganze Geräte wie Drucker, Handys, usw. eingehoben. Leerkassetten wurden früher fast ausschließlich zur Speicherung von Musik oder Videos verwendet. Es kann aber sein, dass auf Speichermedien überhaupt keine urhebergeschützten Werke gespeichert werden (ein geschäftlich genutztes Notebook z.B. oder auch eine Speicherkarte für den eigenen Fotoapparat). Trotzdem wurden diese Geräte über die Leerkassettenvergütung abgabepflichtig. Daher wurden diese Abgaben wiederholt von österreichischen Gerichten als unzulässig erklärt. Amazon versendet z.B. keine strittigen Leermedien oder Geräte mehr nach Österreich um nicht in Gefahr zu kommen, diese Abgabe abführen zu müssen. Um diesen Missstand zu beheben, gibt es ein neues Urheberrecht in Österreich, das die Bundesregierung im Juni 2015 zur Begutachtung vorgelegt hat, und das binnen 10 Tagen beschlossen wird. Darin steht die Speichermedienabgabe nun im Gesetz

Wir sehen die Urheberrechtabgabe als durchaus legitime Abgeltung für die Privatkopie in Österreich. Wir wollen daher die Leerkassettenvergütung reformieren – aber die im neuen Urheberrecht vorgesehene Abgabe auf Festplatten und andere Speichermedien ist das untauglichste aller Mittel dafür.

Die Speichermedienabgabe ist leicht zu umgehen und schadet dem Wirtschaftsstandort Österreich. Der Konsument kann leicht entscheiden seine Speichermedien in Zukunft im Ausland zu kaufen. Bei Amazon konnte man den Kauf im Ausland "in den Griff" bekommen (Amazon verschickt ja seit Jahren keine Speichermedien nach Österreich, um dem Streit über die Urheberrechtsabgabe aus dem Weg zu gehen). Bei tausenden Online-Shops (siehe geizhals.at) im Ausland werden sich die Verwertungsgesellschaften aber schwertun, die Abgabe durchzusetzen.



- Die Speichermedienabgabe ist unfair, da sie in keinsten Weise darauf Rücksicht nimmt, wieviel geschützte Inhalte jemand privat kopiert.
- Die Verdoppelung der Speichermedienabgabe (zu Spitzenzeiten 16 Mio auf 30 Mio) ist nicht zu erklären, wenn gleichzeitig das Recht auf Privatkopie stark beschnitten wurde.
- Ein möglicher Lösungsansatz wäre das Recht auf Privatkopie auf alle privaten, nicht auf Gewinn ausgerichteten Kopien auszudehnen (egal aus welcher Quelle), und als Pauschalabgabe zu etablieren. In diesem Fall wäre auch die o.g. Verdopplung der Abgabe argumentierbar.
- Die Speichermedienabgabe schadet dem Wirtschaftsstandort Österreich, weil sie leicht zu umgehen ist. Konsumenten werden vermehrt dazu übergehen Hardware im Ausland zu kaufen.

7 Datenschutz

Datenschutz ist ein Begriff der nicht ganz einheitlich definiert ist. Er bedeutet Schutz vor missbräuchlicher Datenverarbeitung, Schutz des Rechts auf informationelle Selbstbestimmung, Schutz des Persönlichkeitsrechts bei der Datenverarbeitung oder Schutz der Privatsphäre. Diese Dinge hängen eng miteinander zusammen, haben aber unterschiedliche Bedeutungen. In jeder Bedeutung kommt dem Datenschutz eine wichtige Rolle zu.

7.1 Recht auf informationelle Selbstbestimmung

Dieses Recht bedeutet, dass der Einzelne das Recht hat über die Verwendung seiner Daten selbst zu bestimmen.

7.2 Schutz personenbezogener Daten

Der Schutz von personenbezogenen Daten ist nach Art. 8 der EU-Grundrechtecharta geschützt:

1. Jede Person hat das **Recht auf Schutz der sie betreffenden personenbezogenen Daten**.
2. Diese Daten dürfen nur nach Treu und Glauben für **festgelegte Zwecke** und mit **Einwilligung der betroffenen Person** oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
3. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

In Österreich ist der Datenschutz im [Datenschutzgesetz \(DSG\) 2000](#) geregelt.

7.3 Anwendung des Datenschutzes



In Österreich und in der EU sind die Datenschutzregeln grundsätzlich recht gut. Das Problem, das jedoch besteht, ist, dass sich große Konzerne oft nicht an diese in der EU geltenden Regeln halten. Ein gutes Beispiel dafür ist der Kampf von Max Schrems in Europe vs. Facebook. Max hat nachgewiesen, dass sich Facebook in unterschiedlichsten Bereichen nicht an die geltenden Gesetze hält. Die für die Causa zuständige Datenschutzbehörde ist

Irland, da Facebook dort seinen europäischen Hauptsitz hat (wie viele IT Unternehmen aus steuerlichen Gründen). Die Datenschutzbehörde in Irland ist so klein, dass sie personell nicht einmal in der Lage ist Gesetzesverletzungen nachzugehen. Das nebenstehende Bild zeigt die Datenschutzbehörde in Irland (roter Kreis) – die für die Regulierung von Facebook, Apple, Google, Microsoft und anderen großen Unternehmen innerhalb der EU zuständig wäre, die in Irland ihren Hauptsitz haben. Man kann sich aufgrund des Bildes gut darstellen, dass die Behörde nicht über die Ressourcen verfügt, das auch nur ansatzweise zu erfüllen.



- Europa hat durchaus brauchbare Datenschutzgesetze. Um diese aber auch durchsetzen zu können, braucht es auch schlagkräftige Datenschutzbehörden, die zumindest ansatzweise in der Lage sind, den großen Playern Paroli zu bieten.

7.4 Safe Harbour

Das Safe Harbour Agreement war eine Vereinbarung zwischen Europäischer Union und den USA – bei der die Grundlage dafür geschaffen werden sollte, Daten von europäischen Bürgern in Datenverarbeitungseinrichtungen in den USA verarbeiten und speichern zu können – unter Einhaltung Europäischer Datenschutzregeln. Dieses Abkommen wurde am 6.10.2015 vom EuGH aufgrund einer Klage von Max Schrems für ungültig erklärt, da aufgrund der Massenüberwachung in den USA nicht davon ausgegangen werden konnte, dass die Daten europäischer Bürger ausreichend geschützt seien.

7.5 Passenger Name Record (PNR)

Ein ebenfalls in diesen Bereich – aber auch in den Bereich der Grundrechte – einzuordnendes Thema ist der Schutz von Passagierdaten (kurz PNR oder Passenger Name Record). Dabei geht es darum, wie weitreichende Ermächtigungen die einzelnen Staaten bekommen sollen, auf Passagierdaten zuzugreifen, und welche Informationen von den Fluglinien erhoben werden – und letztendlich dann auch an die Behörden weitergegeben werden müssen. Alexander Sander von der Plattform NoPNR.org beschäftigt sich intensiv mit diesem Thema.

Siehe auch Abschnitt 5.4, Fluggastdaten / Passenger Name Record (PNR)

7.6 ELGA

Auch ELGA (die elektronische Gesundheitsakte) in Österreich ist ein spezieller Fall im Bereich des Datenschutzes. Gesundheitsdaten sind die sensibelsten persönlichen Daten überhaupt. 2013 sorgte ein Skandal von IMS Health für Aufsehen, in dem Ärzte, Spitäler und Apotheken Gesundheitsdaten verkauft hatten¹⁶

In unseren Diskussionen mit den zuständigen Stellen konnten wir bisher nicht überzeugt werden, dass die Gesundheitsdaten, die im ELGA System gespeichert werden, ausreichend vor unzulässigem Zugriff geschützt sind.

Es handelt sich bei ELGA nicht um eine zentrale Speicherung von Patientendaten, sondern vielmehr um eine Vernetzung der Speicherorte. Bereits vorhandene Systeme in Spitälern – werden mit neu geschaffenen Systemen bei Ärzten und Apothekern vernetzt.

¹⁶ <http://diepresse.com/home/panorama/oesterreich/1444211/Was-Aerzte-fur-432-Euro-verkaufen>

Die Funktion der ELGA ist zu begrüßen und das Ziel der ELGA ist es, die Betreuung der Patienten und das Gesundheitssystem generell in Österreich zu verbessern.

ELGA Zugriffe sind insbesondere bei niedergelassenen Ärzten recht gut geschützt. Ein Mediziner kann nur dann auf Patientendaten zugreifen, wenn ein Patient von ihm behandelt wird, und der Patient sich mit seiner E-Card beim Arzt angemeldet hat.

Problematischer scheint die Situation überall anders zu sein. Z.B. in Spitälern wird der Zugriff auf ELGA auch ohne Vorliegen der E-Card erlaubt – und zwar für alle Spitalsmitarbeiter im Spital in dem der Patient behandelt wird. Jeder Zugriff auf Patientendaten wird zwar protokolliert und unbefugter Zugriff unter strenge Strafen gestellt. Wir wissen jedoch bereits von anderen Systemen, dass eine Protokollierung und Strafandrohung Täter nicht von einem Datendiebstahl abhalten wird¹⁷. Für einen Patienten wird es unmöglich sein, festzustellen ob Hr. Müller oder Frau Mayer im Spital auf seine Daten zugreifen dürfen. Denn er kennt die Mitarbeiter aus dem Labor, die sein Blutbild machen nicht.

Ebenso gibt es im System keinerlei Einschränkungen nach Fachgebieten. Es wird sicherlich für eine Zahnbehandlung unerheblich sein, ob der Patient soeben wegen eines Fußpilzes oder einer Geschlechtskrankheit in Behandlung war

Patienten können zwar einzelne Befunde ein- und ausblenden. Der Patient wird sich jedoch nicht wegen jedes einzelnen Arztbesuches oder einem (vielleicht ungeplanten) Spitalsaufenthalt überlegen welche einzelnen Befunde er in Zukunft ausblenden will.

Ein weiterer Kritikpunkt betrifft die Benutzbarkeit des online Systems. Weniger als 10% der Bevölkerung besitzen derzeit eine Bürgerkarte/Handy Signatur. Nur mit dieser ist der Zugriff auf das ELGA System für einen Patienten möglich. Damit können derzeit – mangels Verbreitung der Handysignatur 90% der Bevölkerung noch nicht auf ELGA zugreifen.

¹⁷ <http://www.vol.at/prozess-um-illegale-abfragen-im-polizeicomputer-vier-monate-bedingt/3247950>

Positiv zu erwähnen ist, dass sich Patienten dazu entscheiden können komplett aus ELGA auszusteigen. Für die über 90% der Bevölkerung die derzeit das Online System (wegen fehlender Handysignatur) nicht nutzen können ist eine schriftliche Abmeldung¹⁸ möglich. Idealer wäre sicherlich hier ein Opt-In System gewesen. Dann hätte sich die ELGA GmbH mehr anstrengen müssen die Patienten von ihrem System zu überzeugen.



- Gesundheitsdaten sollten generell nur verschlüsselt gespeichert werden dürfen, da sie zu den sensibelsten Daten überhaupt zählen (nicht nur für ELGA).
- Der Patient sollte volle Kontrolle über jeglichen Zugriff auf seine Befunde und Daten haben. Ein Zugriff sollte daher nur durch willentliches Einverständnis des Patienten möglich sein. (Stecken der E-Card).
- Notfallsdaten (Blutgruppe, Allergien) können auf Wunsch des Patienten unverschlüsselt hinterlegt werden.
- Die ELGA sollte nach Fachgebieten unterteilt werden. Mediziner sollten nur relevante Informationen angezeigt bekommen.
- Der Schutz des Onlinesystems durch Handysignatur / Bürgerkarte ist gut. Jedoch muss hier in die Akzeptanz des Systems durch die Bevölkerung investiert werden. Lediglich unter 10 Prozent der Österreicher verfügen über eine Handy Signatur - daher ist die massive Verstärkung der Einrichtungen und Ausstattung der Patienten-anwaltschaft erforderlich.

¹⁸ <https://www.gesundheit.gv.at/Portal.Node/ghp/public/content/help/hilfe-formularservice.html>

7.7 E-Call

Auch das neue Auto-Notrufsystem E-Call, das ab März 2018 verpflichtend in alle Neuwagen verbaut werden muss, ist ein Thema. Zum einen wird E-Call angepriesen, dass es in Zukunft Leben retten wird, wenn ein Auto automatisch die Notdienste verständigt, wenn ein Unfall passiert ist; zum anderen macht es ein Auto aber auch zum perfekten Datensammler, wenn nicht ausreichend geregelt wird, wer wie auf die Daten des E-Call Systems zugreifen darf.

Es gibt derzeit keine Möglichkeit E-Call als Autofahrer zu verhindern. Der Fahrer sollte selbst darüber entscheiden können, ob er das System nutzen möchte – vor allem so lange die datenschutzrechtlichen Bedenken nicht geklärt sind.



- E-Call kann durch die Verständigung von Notfallorganisationen entscheidende Zeit sparen um Leben zu retten.
- Es müsste aber garantiert werden, dass die Daten der in den Autos verbauten Handys nicht gesammelt und weiterverwendet werden. (Stichwort Bewegungsprofile)
- Besonders problematisch würde das System im Zusammenhang mit einer Vorratsdatenspeicherung und dem Zugriff von Geheimdiensten auf solche Daten.

7.8 Smartmeter

Auch die neuen "intelligenten" Stromzähler fallen unter die Kategorie des Datenschutzes und sind heftig umstritten. Derzeit beginnen die Stromversorger in Österreich die Zähler durch elektronisch ablesbare und steuerbare Geräte auszutauschen.

Die neuen Stromzähler verraten durchaus einiges über die Bewohner von Wohnungen und Häusern. Es gibt Bedenken, dass die Informationen missbraucht werden können, genauso wie es massive Sicherheitsbedenken (Siehe dazu Punkt 9.3) gegen den Einsatz solcher Geräte gibt. Für den Konsumenten ergeben sich durch dieses neue System jedoch keine Vorteile.

In Österreich gibt es zwar eine Opt-Out Möglichkeit. Es hat sich aber gezeigt, dass Energieversorger davon nichts wissen, oder wissen wollen. Zudem wird trotzdem ein intelligenter Zähler verbaut, die Intelligenz aber abgeschaltet (was für den Konsumenten kaum kontrollierbar ist). In Deutschland ist man mittlerweile von der flächendeckenden Umstellung wieder abgekommen, weil ein entsprechender Nutzen nicht darstellbar war.



- Smartmeter haben für den Kunden den einzigen Nutzen, dass er den Zähler nicht mehr selbst ablesen muss.
- Auch für die Netzbetreiber scheinen die Vorteile nicht so groß zu sein, dass eine flächendeckende Umstellung Sinn hat. In Deutschland ist man davon wieder abgerückt.
- Sollten derartige Stromzähler zum Einsatz kommen, müssten entsprechende Vorkehrungen getroffen werden, dass die Zuordnung zu Personen nicht möglich ist und die Verwendung der Daten genau definiert werden.
- Auch die Sicherheitsaspekte (Hackerangriffe) auf die Zähler und unbefugtes Ein- / Ausschalten der Stromversorgung sind noch nicht restlos geklärt.

8 Transparente öffentliche Verwaltung

Die Digitalisierung hat auch in der öffentlichen Verwaltung Einzug gehalten. Dass nun viele Prozesse im Staat elektronisch abgewickelt werden, bedeutet nicht nur eine Vereinfachung für den Staat und die Bürger, sondern auch die Möglichkeit für den Staat transparenter für seine Bürger zu werden – und diese auch aktiver in Entscheidungsprozesse einzubinden. Transparenz schafft mehr Vertrauen – und eine aktive Einbindung in die Prozesse schafft auch ein Gemeinschaftsgefühl.

Im Artikel 1 des Österreichischen Bundesverfassungsgesetzes heißt es:

Österreich ist eine demokratische Republik. Ihr Recht geht vom Volk aus.

Um es anders auszudrücken: Wir sind der Staat. Die Bürger des Staates zahlen Steuern. Mit diesem Geld wird der Staat aufrechterhalten. Verwaltet wird der Staat von den 3 Staatsgewalten – Der Exekutive (ausführende Gewalt), der Legislative (Gesetzgebung) und der Judikatur (Rechtsprechung).

Da es in früherer Zeit vollkommen unmöglich war, das Volk gesamtheitlich zu befragen, gibt es Intermediäre wie politische Parteien und Verbände sowie Medien als Bindeglied zwischen dem Volk und der Verwaltung des Staates.

8.1 Verwaltungstransparenz

Bei der Verwaltungstransparenz geht es darum, dass die Bürger Einblick in die Verwaltungsvorgänge und Entscheidungsprozesse des Staates bekommen. Bei der Entwicklung hin zur transparenten Verwaltung unterscheidet man 4 Stufen:

1. Der Staat stellt ausgewählte allgemeine Informationen zur Verfügung
2. Der Staat gewährt Einblick in die Verwaltungsvorgänge die den jeweiligen Bürger betreffen
3. Der Staat gewährt Einblick in alle Vorgänge, eine Betroffenheit muss nicht gegeben sein
4. Der Staat unterstützt den Bürger aktiv bei der Einsicht in Verwaltungsvorgänge und vermittelt auch proaktiv notwendige Hintergrundinformationen und Fähigkeiten

Ziel ist es, das Vertrauen der Bürger in ihre Verwaltung und den Staat zu stärken und auch dem Volk selbst eine Kontrollmöglichkeit zu geben.



- Der Staat sollte gegenüber seinen Bürgern transparent sein. Es sollte dem Bürger möglich sein, die Vorgänge innerhalb der Verwaltung zu verstehen und nachvollziehen zu können.
- Diese Transparenz erhöht den Druck auf den Staat im Sinne der Steuerzahler (Firmen und Privatpersonen) zu agieren.
- Für den Bürger steigert die Transparenz das Vertrauen in den Staat und dessen Institutionen.

8.2 Digitale Demokratie / E-Democracy

Früher war es unabdingbar, Volksvertreter damit zu beauftragen an einen Ort zu reisen und dort ihre Wähler zu repräsentieren. Wir sprechen darum auch von einer repräsentativen Demokratie. Heute wäre es theoretisch technisch möglich eine vollständig direkte Demokratie auszuüben. Abstimmungen könnten elektronisch unterstützt durchgeführt werden. Ein Umbruch von einer repräsentativen Demokratie direkt in eine digitale Demokratie – oder E-Democracy – ist nicht wahrscheinlich, dennoch sind Hybrid Szenarien mit einer stärkeren Bürgerbeteiligung durchaus denkbar und wünschenswert. Damit das Volk aber direkter in demokratische Entscheidungsprozesse eingebunden werden kann, müsste der Staat zuerst transparenter und das Volk auch aktiv mit den notwendigen Informationen versorgt werden, um solche Entscheidungen überhaupt treffen zu können.

Eine solche hybride Form ist die Liquid Democracy.



- Eine aktivere Einbindung der Bürger in Entscheidungsprozesse erfordert aber, dass Bürger ausreichend informiert werden, um überhaupt in der Lage zu sein, derartige Entscheidungen zu treffen.
- Ein Problem der direkten versus der repräsentativen Demokratie ist, dass Bürger dazu tendieren, Regelungen die ihnen persönlich schaden, aber der gesamten Öffentlichkeit nutzen abzulehnen.
- Um Bürger direkter einbinden zu können, müssen auch entsprechende Strukturen und Technologien zur Verfügung stehen, die es auch wirklich allen erlauben teilzunehmen.

8.3 E-Government

Unter E-Government versteht man die Nutzung digitaler Technologien für die Verwaltung des Staates. Beispiele dafür sind Finanz Online oder die Elektronische Gesundheitsakte ELGA.

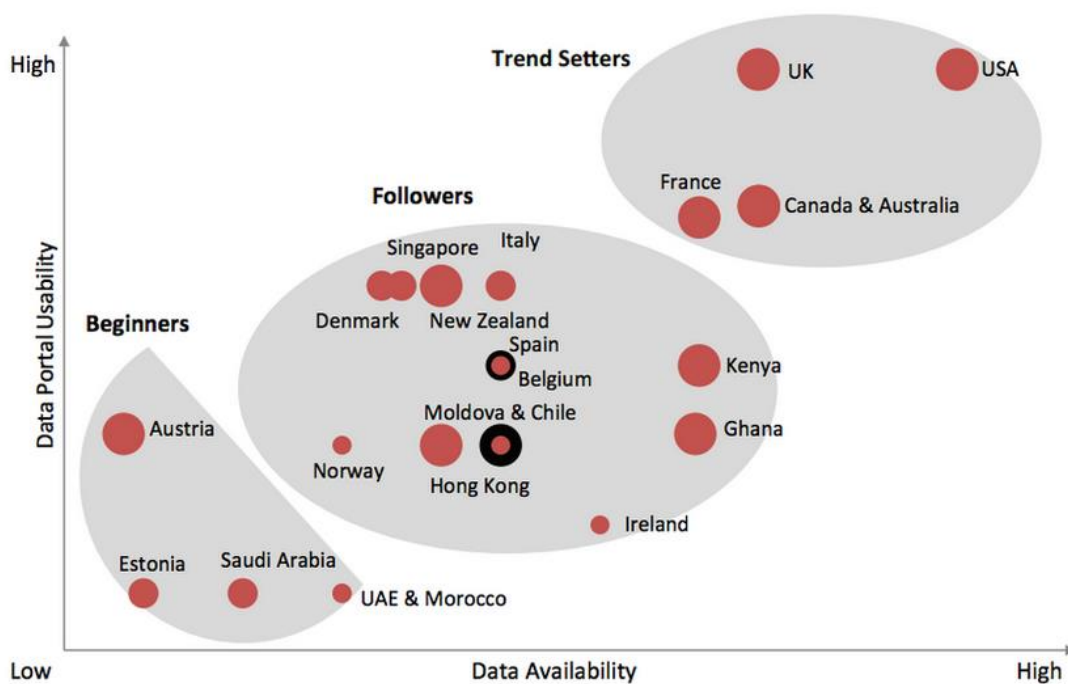


- E-Government Angebote haben sich in letzter Zeit bereits deutlich verbessert, es gibt hier aber noch sehr viele Bereiche, die noch überhaupt nicht abgedeckt sind.
- Für ein für alle verwendbares Government muss auch daran gearbeitet werden, dass alle teilnehmen können. So verwenden z.B. derzeit nur unter 10% der Bevölkerung die Bürgerkarte in Form der E-Card bzw. Handysignatur. Es müssen daher alle Dienste und Informationen der öffentlichen Verwaltung auch für die „Bewohner der anderen Seite der digitalen Kluft“ ohne Barrieren und (zusätzliche) Kosten zugänglich bleiben. Durch die Digitalisierung der Verwaltung dürfen keine Bürger 2.Wahl (denen die Errungenschaften der „Digitalen Welt“ nicht zugänglich/leistbar sind) generiert werden.

8.4 Open Data

Open Data bedeutet die freie Nutzbarkeit von Daten, die vom Staat erhoben werden. Da das Volk die Erhebung solcher Daten finanziert, scheint es auch nur logisch zu sein, dass diese Daten wiederum allen zur Verfügung stehen sollten. Open Data ist auch eng verbunden mit Verwaltungstransparenz, denn wenn die entsprechenden Daten zur Verfügung gestellt werden, dann ist das ein erster Schritt für eine vollständig transparente öffentliche Verwaltung.

Österreich hat hier laut einer Studie von Cap Gemini durchaus noch einiges an Aufholbedarf. Österreich wird hier in der Studie als Beginnerland eingestuft, auf gleicher Stufe mit den Vereinigten Arabischen Emiraten, Dubai und Estland:



Note: Size of bubble represents level of government support.

Source: Capgemini Consulting Analysis

Laut dem [Global Open Data Index 2015](http://index.okfn.org/place/austria/)¹⁹ liegt Österreich auf Platz 23. Hier die Detailergebnisse:

¹⁹ <http://index.okfn.org/place/austria/>

Rank	Dataset	Breakdown	Location (URL)	Format	Info	Prev. (2014)	Score
1	National Statistics	         	http://data.statistik.gv.at/we...	PDF, ...		#23 70%	100%
1	National Map	         	http://www.basemap.at/	Web ...		#1 100%	100%
1	Election Results	         	http://www.data.gv.at/nrw2013	CSV		#1 100%	100%
7	Legislation	         	https://www.ris.bka.gv.at/defa...	HTML, ...		#6 90%	90%
8	Government Spending	         	n/a	n/a		#15 10%	10%
36	Procurement tenders	         	https://www.auftrag.at/WZOnlin...	n/a		n/a	45%
36	Location datasets	         	n/a	n/a		#30 35%	25%
36	Land Ownership	         	n/a	n/a		n/a	20%
38	Water Quality	         	http://www.trinkwasserinfo.at/...	n/a		n/a	30%
45	Government Budget	         	https://www.bmf.gv.at/budget/d...	xls		#43 55%	60%
47	Company Register	         	http://www.justiz.gv.at/web201...	n/a		#26 45%	25%
62	Pollutant Emissions	         	http://www.umweltbundesamt.at/...	n/a		#51 35%	30%
69	Weather forecast	         	https://www.zamg.ac.at/cms/en/...	n/a		n/a	20%

Besonders schlecht schneidet Österreich in der Verfügbarkeit der Daten über öffentlichen Ausgaben und der Grundbuchdaten ab.

9 Infrastruktur

Die Infrastruktur, auf die die "digitale" Welt aufbaut, besteht vor allem aus Strom und dem Internet sowie den Rechenzentren. Das Internet wurde ermöglicht durch eine Zusammenarbeit aus Forschungseinrichtungen, dem Militär und Firmen für die die Politik die entscheidenden Voraussetzungen geschaffen hat.

Ohne eine sichere und für alle zugängliche Infrastruktur können wir vom digitalen Wandel nicht profitieren. Es ist daher wichtig, dass das Netz weiterhin für alle offen und zugänglich bleibt, und dass vor allem auch die Sicherheit des Netzes wiederhergestellt wird. Auch die Sicherheit der gesamten kritischen Infrastruktur benötigt mehr Aufmerksamkeit als derzeit.

Wir empfinden es hier als wichtig, dass sich Infrastruktur-Politiker eine unabhängige Meinung bilden und sich nicht von Telekom Providern vor den Karren spannen lassen.

9.1 Frei verfügbares und neutrales Internet

Das Internet wurde als Verbindung von unabhängigen miteinander verbundenen Netzen konzipiert. Das Internet gehört niemandem und funktioniert nur, weil alle teilnehmenden Netze den anderen Teilnehmern dessen Nutzung erlauben. Das Internet ist zusätzlich ein neutrales Netz. Das Netz ist agnostisch gegenüber den darauf laufenden Anwendungen und Daten (Netzneutralität). Das macht den Erfolg des Netzes aus. Genau diese beiden Eigenschaften sind nun in Gefahr. Die Betreiber des Internet sind mittlerweile die großen Telekom Carrier, die natürlich mit dem Betrieb des Netzes Geld verdienen und möglichst andere Betreiber an den Rand drängen wollen, um den Profit zu optimieren. Dabei werden immer neue Methoden gefunden, um gewisse Dienste im Netz zu bevorzugen oder die freie Nutzung einzuschränken. Das gefährdet insgesamt die Digitalisierung und auch Europa als Wirtschaftsstandort. Denn die USA ist uns hier in weiten Bereichen wesentliche Schritte voraus.

9.2 Zugängliches Internet

Das Internet entwickelt sich immer mehr zur universellen Kommunikationsplattform. Es muss darauf geachtet werden, dass das Internet für alle Bevölkerungsschichten und Personengruppen zugänglich ist. Unter diesen Aspekt fallen sowohl die Beseitigung von Zugangsschranken wie z.B. unzureichendes technisches Wissen, kommerzielle Probleme (derzeit gibt es eine Telefon- Grundgebührenbefreiung und eine Befreiung von der GIS Gebühr. In Zukunft sollte man überlegen, ob nicht das Internet den Platz von Telefon und Fernsehen übernommen hat). Aber auch persönliche Einschränkungen wie z.B. die Benutzbarkeit von Websites und anderen Applikationen durch Blinde.



- Um in der digitalen Welt partizipieren zu können benötigt man ein entsprechendes Gerät (Smartphone, Tablet, PC) und einen Zugang zum Netz.
- Dafür ist es notwendig etwaige wirtschaftliche Hürden zu eliminieren. Eine Förderung / Zuschuss für Internet Zugänge für benachteiligte Bevölkerungsgruppen (z.B. Grundgebührenbefreiung für Internet statt für Festnetz-Telefonie alleine) wäre sinnvoll.
- Es müssen aber auch die technologischen Hürden überwunden werden. Hier ist eine entsprechende Unterstützung (Schulungen, Selbsthilfegruppen, Erwachsenenbildung) notwendig.
- Auf Bevölkerungsgruppen mit persönlichen Einschränkungen (wie z.B. Blinde) muss besonders geachtet werden. Trotz entsprechenden Gesetzen sind viele Angebote noch immer nicht vollständig zugänglich.
- Eine freie Zugänglichkeit bedeutet auch, dass Internet flächendeckend verfügbar sein muss. (siehe Breitbandausbau)

9.3 Sicherheit der Infrastruktur

Ein weiterer Punkt ist, dass durch die Digitalisierung der Infrastruktur viele kritische Systeme auch mit dem Internet verbunden sind und darüber gesteuert werden können. Das ist positiv – weil viele Aufgaben erleichtert werden.

Was aber, wenn der Schutz dieser Systeme unzureichend ist? Dann können solche Steuerungsfunktionen auch von Personen durchgeführt werden, die dazu nicht ermächtigt wurden (z.B. Hacker oder noch schlimmer: Terroristen). Was ist, wenn zum Beispiel ein Unbefugter Kraftwerke abschaltet oder Smartmeter nicht dazu verwendet den Strombedarf abzulesen, sondern ganzen Häusern oder Industrieanlagen die Energieversorgung abzuschalten? Was würde geschehen, wenn jemand in der Hauptverkehrszeit alle Ampeln auf Grün schaltet?

Was, wenn der Geheimdienste wie NSA oder GHCH einfach alle Daten, die auf den Kabeln übertragen werden, einfach mitliest oder sich in kritische Unternehmungen einhackt und deren Sicherheit kompromittiert (wie z.B. beim SIM Karten Hersteller Gemalto)? Der Gemalto Hack hatte zum Beispiel die Konsequenz, dass die Verschlüsselung der Mobilfunktechnologie keinen Wert mehr hat. Auch das Vertrauen in US Hersteller wie CISCO wurde kompromittiert, weil bekannt wurde, dass der Geheimdienst Equipment am Versandweg zum Kunden abgefangen und präpariert hat.

Was hat das alles für die Nutzbarkeit der Infrastruktur für Unternehmen zu bedeuten? Kann das Internet überhaupt noch verwendet werden, um sensible Daten zu übermitteln? Kann man die Mobiltelefonie überhaupt noch für heiklere Kommunikation im geschäftlichen Umfeld nutzen? Oder ist es notwendig wieder komplett getrennte Systeme zu schaffen um wieder entsprechende Sicherheit zu erlangen? Es ist mittlerweile erwiesen, dass die Geheimdienste vor allem auch **Industriespionage** betreiben. Unternehmen müssen sich gegen derartige Angriffe schützen, sonst verlieren sie im Wettbewerb.

Auch **Cyberattacken** zwischen Staaten sind mittlerweile, spätestens seit dem Stuxnet Angriff der USA auf die Zentrifugen des Irans, öffentlich bekannt. Aber auch zwischen China und den USA tobt derzeit ein Krieg im Cyberspace.

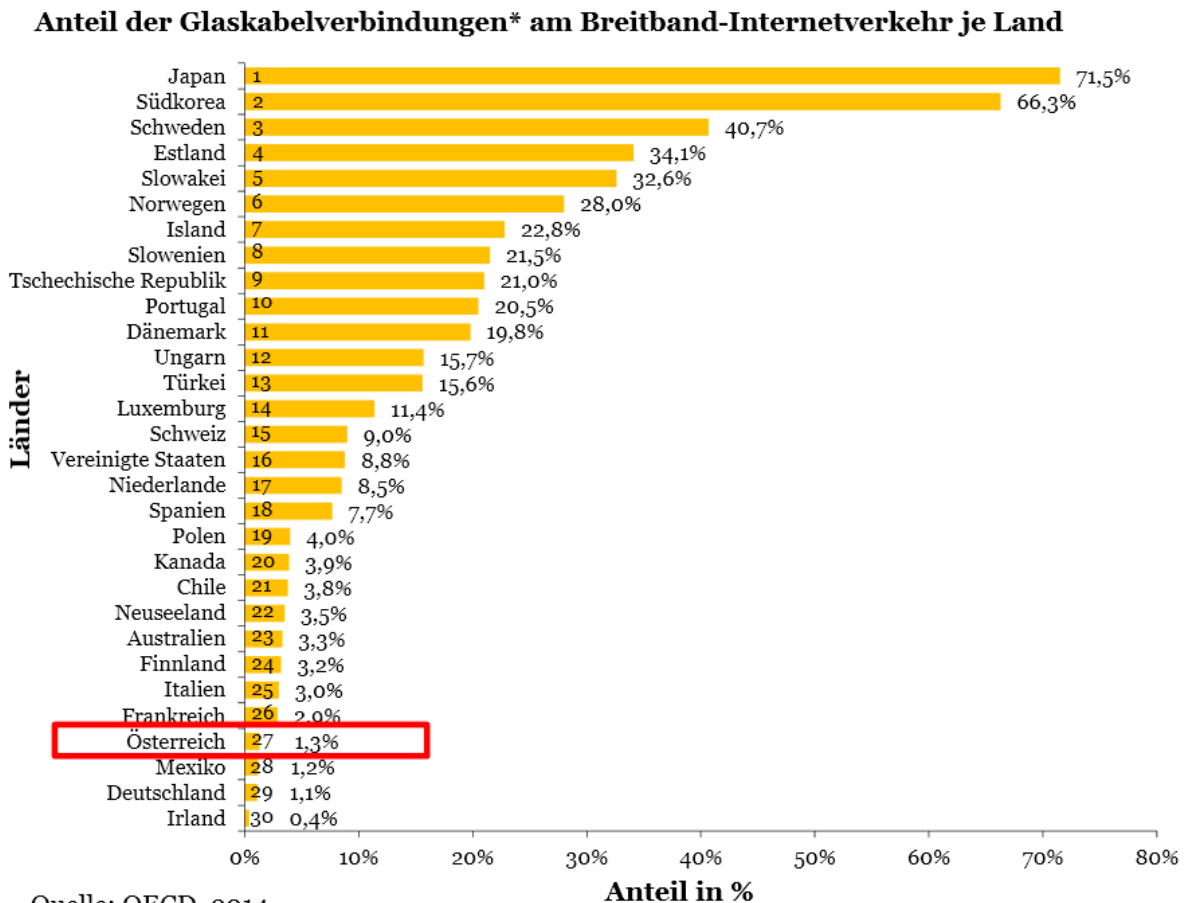


- Die Sicherheit und das Vertrauen in Netz und Hersteller muss wiederhergestellt werden.
- Vor allem Industriespionage, aber auch politisch motivierte Spionage gefährden den Europäischen Wirtschaftsstandort.
- Es muss im Interesse der Länder und der EU sein, hier eigene Kapazitäten aufzubauen und sich nicht auf die „Hilfe“ von außen zu verlassen.
- Hersteller haben ebenfalls Interesse das Vertrauen in Ihre Produkte wiederherzustellen. Initiativen wie das Microsoft Transparency Center zeigen, dass Hersteller Einblick in ihre Produkte gewähren, um die Skepsis vor dem Einsatz der Produkte zu nehmen.

9.4 Breitbandausbau

Wenn wir uns die Infrastruktur-Netze in Österreich ansehen, dann sehen wir, dass in den letzten Jahren das Netzwerk von den Diensten getrennt wurde. Nehmen wir beispielsweise die ÖBB. Die ÖBB wurde in das (Schienen-)Netzwerk (ÖBB Infrastruktur AG) und in Personen- und Güterverkehr getrennt. Die ÖBB Infrastruktur AG bietet das Schienennetz zu gleichen Konditionen der ÖBB Personenverkehrs AG wie auch der Westbahn, die ein Mitbewerber der ÖBB ist, an. Das fördert den Wettbewerb im Bahnverkehr. Es wäre wohl ziemlich unvernünftig, wenn die Westbahn einen eigenen Schienenstrang von Wien nach Linz bauen müsste, um ebenfalls Personenzüge zwischen den beiden Städten verkehren zu lassen. Die gleiche Trennung gab es beim Strom (Wiener Netze / Wienstrom), beim Gas, etc. Der einzige Bereich in dem diese Trennung nicht erfolgt ist, ist der Telekommunikationsbereich.

Österreich liegt beim Ausbau breitbandiger Internet Anschlüsse, die fast ausschließlich über Glasfaser realisiert werden können, weit zurück:



Um einen vernünftigen Wettbewerb in der Telekommunikationsinfrastruktur zu ermöglichen, muss der Glasfaserausbau so rasch als möglich vollzogen werden. Viel Fördergelder in „tote Technologie“ (Kupfer) zu investieren nützt zwar den Telekom Anbietern die große Kupfernetze haben, aber nicht der Gesellschaft.

Eine intensive Zusammenarbeit mit anderen Infrastruktur-Errichtern wie Straße, Strom, Kanal, ... ist unabdingbar, um hier rasch und auch kosteneffizient den Rückstand aufzuholen.



- Wir glauben, dass nur durch Trennung des Netzbetriebs von den darauf laufenden Diensten ein fairer Wettbewerb im Netz hergestellt werden kann.
- Infrastrukturförderungen sollten dazu führen, dass Netzbetreiber ihr Netz für Mitbewerber öffnen müssen. (Stichwort Breitbandmilliarde).
- Betreiber, die im Eigentum der öffentlichen Hand stehen, sollten ebenso verpflichtet werden, ihr Netz für andere zu öffnen. (z.B. Energienetzbetreiber).
- Gemeinden und Länder sollen dazu verpflichtet werden, bei jeder Grabungsarbeit Leerverrohrungen herstellen zu müssen.

9.5 Netzneutralität

Netzneutralität bedeutet, dass ein Netzbetreiber sich neutral gegenüber in seinem Netz übertragenen Daten verhält. D.h., dass er alle Daten gleichbehandelt, egal um welche Daten es sich handelt.

Für die Digital Society ist dieses Thema sehr wichtig, denn es ist einer der Grundpfeiler des Erfolges des Internets. Ohne Wahrung der Netzneutralität droht das Internet wieder zu einem geschlossenen System zu werden.

In der EU wurde ein Gesetzesentwurf erarbeitet, der das Roaming innerhalb der EU abschafft (telefonieren innerhalb der EU Länder muss überall gleich teuer sein – ähnlich wie die Bankomat Behebungen) – das kommt vor allem Firmen zugute, die viele Mitarbeiter haben, die im Ausland telefonieren. Gleichzeitig wird die EU erlauben, dass für "Spezialdienste" (der Begriff wird nicht genauer definiert) – die Provider extra Gebühren einheben dürfen. D.h., in Zukunft ist es möglich, ein Internet ohne z.B. YouTube oder Netflix zu bekommen. Wer Videos Streamen möchte, muss dafür extra zahlen. Wie das Internet in Zukunft aussehen könnte zeigt dieses Bild:



DIE NEUEN DSL-OPTIONEN 2016 ENTDECKE DIE GRENZENLOSE FREIHEIT

NEUE FLATOPTIONEN
FÜR JUNGE LEUTE!



Im Oktober 2015 hat das Europaparlament Regeln zur Netzneutralität beschlossen. In diesen Regeln wurde die Netzneutralität, wie sie bisher gelebt wurde, abgeschafft. Es werden sogenannte "Spezialdienste" zugelassen. Man kann also in Zukunft dafür bezahlen (oder muss), um ein qualitatives Internet zu bekommen.

In ersten Reaktionen haben die Deutsche Telekom sowie auch Drei in Österreich aufhorchen lassen, die in einem "Förderprogramm" für neu gegründete Unternehmen angeboten haben, gegen „ein paar Prozent vom Umsatz“²⁰ solchen Unternehmen dann auch ein verwendbares Internet zur Verfügung zu stellen. Im Internet wurde diese Vorgehensweise dann mit Schutzgelderpressung bzw. Raubrittertum verglichen. Wenn man in Zukunft nicht bereit ist, für einen vernünftigen Zugang zum Internet mehr zu bezahlen, dann wird der Anschluss vom Provider einfach so heruntergeregelt, dass er nicht mehr verwendbar ist. Genau davor hatten die Kritiker der Regelung gewarnt.

In Österreich haben alle im Europaparlament vertretenen Parteien die neue Regelung abgelehnt. Nur die ÖVP Fraktion hat dem Vorschlag zugestimmt. MEP Dr. Paul Rübig, der für die Position der ÖVP Fraktion verantwortlich zeichnet, erklärt [seinen Standpunkt auf seiner Website](#)²¹. Es ist schade, dass gerade die Wirtschaftspartei ÖVP sich hier gegen die österreichischen Wirtschaftstreibenden stellt, und den Wirtschaftsstandort Österreich gegenüber den USA noch mehr ins Hintertreffen geraten lässt.

Die USA ist Europa in diesem Bereich weit voraus. Denn die FCC (Commission) hatte das Prinzip der Netzneutralität im Februar 2015 festgeschrieben. ([siehe Bericht der BBC](#))²²

9.5.1 Beispiele für Verletzungen von Netzneutralität

Spiegel: [Bürgerrechtler kritisieren Internet.Org](#)²³

Internet.org es, weil diese Menschen nur noch das vorgesetzt bekommen, was Marc Zuckerberg zulässt. an. Damit können Inhaber einer SIM Karte eines bestimmten Providers gratis auf Facebook, Wikipedia und eine Auswahl an Seiten gratis zugreifen. So toll es ist, dass ärmere Bevölkerungsschichten bestimmte Services benutzen können, so gefährlich ist es, weil diese Menschen nur noch das vorgesetzt bekommen, was Marc Zuckerberg zulässt.

²⁰ <http://derstandard.at/2000024736135/Netzneutralitaet-Deutsche-Telekom-will-Umsatzbeteiligung-von-Start-ups>

²¹ <http://www.paulruebig.eu/presse-news/pressemitteilungen/1443-wording-zum-thema-netzneutralitaet>

²² <http://www.bbc.com/news/technology-31638528>

²³ <http://www.spiegel.de/netzwelt/netzpolitik/facebook-initiative-aktivisten-kritisieren-internet-org-a-1034428.html>

ORF FM4: Drei Spotify und die Netzneutralität²⁴

Der Mobilfunkanbieter Drei bietet bei einem Tarif die Möglichkeit an, dass über Spotify gehörte Musik nicht zum vom Kunden verbrauchten Datenvolumen gezählt wird (Diese Praxis nennt man Zero-Rating). Auf der einen Seite ist das natürlich für den Nutzer positiv, auf der anderen Seite schließt Drei damit potentielle Mitbewerber von Spotify aus. Sie können im Netz von 3 nicht mehr mit Spotify konkurrieren. Wenn ich für den einen Dienst Datenvolumen verrechnet bekomme, für einen anderen aber nicht, dann ist klar, dass der Konsument nur noch Spotify verwenden wird. Das verzerrt den Wettbewerb.



- Netzneutralität ist die Grundvoraussetzung für die Innovationskraft im Internet.
- Die großen Telekom Carrier versuchen natürlich alles, Mitbewerber aus ihren Netzen herauszuhalten und genau das muss verhindert werden.
- Eine verpflichtende Trennung des Netzbetriebes von den darauf laufenden Diensten würde das Problem unmittelbar und endgültig lösen.

²⁴ <http://fm4.orf.at/stories/1741685/>

10 Andere Institutionen

10.1 Private Vereine / Zivilgesellschaft

10.1.1 Verein der Internet Benutzer VIBE



Der "Verein für Internet-Benutzer Österreichs (VIBE.AT)" wurde Anfang 1999 infolge von Diskussionen im Usenet gegründet, um die Interessen der Benutzer gegenüber Behörden, Internet-Service-Providern (ISPs) und anderen Organisationen zu vertreten.

Web: <https://www.vibe.at>

Obmann: Andreas Krisch

10.1.2 AK Vorrat



Der Arbeitskreis Vorratsdatenspeicherung (kurz AKVorrat) wurde gegründet, um sich gegen die Einführung der Vorratsdatenspeicherung in Österreich und Europa einzusetzen.

Web: <https://www.akvorrat.at>

Präsident: Christof Tschohl, Geschäftsführer: Thomas Lohninger

10.1.3 Open3



Der Verein Open3 steht für Open Society, Open Government und Open Data – die drei Dimensionen, die in einem modernen Staat zu hoher **Transparenz, Partizipation** und **Partizipationsfähigkeit** und Möglichkeiten der **Kollaboration** zwischen verschiedenen Stakeholdern führen.

Web: <https://www.open3.at/>

Obmann: Robert Harm

10.1.4 Österreichische Computer Gesellschaft



**OESTERREICHISCHE
COMPUTER GESELLSCHAFT**
AUSTRIAN
COMPUTER SOCIETY

"Wir bauen Brücken - von der Wissenschaft über die Wirtschaft zur Arbeitswelt."

Die Österreichische Computer Gesellschaft) ist ein gemeinnütziger Verein zur Förderung der Informationstechnologie unter Berücksichtigung ihrer Wechselwirkungen mit Mensch und Gesellschaft. Der Verein bietet ein interdisziplinäres Forum für aktuelle IT-Themen. Er ist ein wichtiger und ernst genommener Dialogpartner und Themensetzer für gesellschaftspolitisch relevante IT-Themen.

Die OCG bietet ein Forum für Networking, ist eine kompetente sowie verlässliche Partnerin im Bereich der Veranstaltungsorganisation und fördert damit Beziehungen zwischen Wissenschaft und Wirtschaft. Darüber hinaus bietet sie ein standardisiertes, unabhängiges und qualitatives Weiterbildungsangebot im IT-Bereich und schlägt damit eine wichtige Brücke zur Arbeitswelt.

Web: <http://www.ocg.at>

Präsident: Mag. Markus Klemm

10.15 Forum für Informationsfreiheit (FOI)



Ziel des Vereins ist die Stärkung der Informationsrechte der Bürgerinnen und Bürger sowie der Öffentlichkeit gegenüber staatlichen Institutionen. Davon erfasst sind

sowohl die Tätigkeit der Legislative, Exekutive und Jurisdiktion sowie der Privatwirtschaftsverwaltung und öffentlicher Versorgungsunternehmen.

Web: <https://www.informationsfreiheit.at/>

Vorstand: Josef Barth, Tanja Malle, Markus Hametner

10.16 Forum Datenschutz



Das Forum Datenschutz will ein umfassendes Informations-, Beratungs- und Unterstützungsangebot für Fragen des Datenschutzes schaffen.

Seminare und Beratungsangebote sollen einem möglichst breiten Kreis von NutzerInnen und Unternehmen zugänglich werden. Als Verein versteht sich das Forum Datenschutz dabei als Vermittler zwischen NutzerInnen und Unternehmen.

Web: <https://forumdatenschutz.at>

Vorstand: DI Alice Sedmidubsky / Mag. Andreas Krisch

10.17 Neuwal.com



neuwal.com

neuwal – Politik- und Wahljournal ist ein privates und unabhängiges Projekt zur Förderung der politischen Bildung. Wir berichten seit 2008 mit

derzeit mehr als 10 aktiven JournalisteInnen und BloggerInnen unparteiisch und unabhängig über politische, gesellschaftliche und wirtschaftliche Entwicklungen.

Web: <https://neuwal.com>

Obmann: Dieter Ziernig – Mitarbeiter: Robert Harm

10.18 Qualitätszeit.at



Die sogenannten „Digitalen Medien“ sind heutzutage zu essentiellen Begleitern im Alltag

geworden. Für viele ist der Umgang mit Internet, Smartphone und Co. selbstverständlich. Dennoch wissen längst nicht alle Menschen, wie sie die neuen Technologien effektiv nutzen können. Oft liegt dies an der Angst, „etwas kaputt zu machen“, aber vor allem an der fehlenden Unterstützung bei der Nutzung.

qualitätszeit setzt sich aktiv für eine Förderung von individuellen Mediennutzungskompetenzen ein.

Verein für Medienarbeit und Generationen

Web: <http://www.qualitaetszeit.at/>

Vorsitzende: Mag. Daniela Weinholtz

10.19 Digitalista.at



Digitalista setzt es sich zum Ziel, Frauen in der österreichischen Digital-Branche beruflich und persönlich zu fördern.

Unsere Mission ist es, Frauen in der Digital-Branche in ihrer beruflichen und persönlichen Weiterentwicklung zu fördern. Durch die Arbeit von Digitalista sollen österreichische Onlinerinnen Selbstbewusstsein für ihre Position entwickeln und an ihrer Karriere arbeiten. Zudem ist es Ziel von Digitalista, mehr Frauen in Führungspositionen zu bringen.

Digitalista – Initiative zur Förderung von Frauen in der österreichischen Digital-Branche.

Web: <http://digitalista.at>

Obfrau: Elisabeth Oberndorfer



10.110 Open Knowledge Austria



Die Open Knowledge Foundation Österreich setzt sich für offene Daten, freies Wissen, Transparenz und Beteiligung ein. Um diese Ziele zu erreichen, engagieren wir uns öffentlich für diese Themen und entwickeln einschlägige Technologien, Trainings, Projekte und Veranstaltungen. Die gemeinnützige

Organisation ist Teil eines internationalen Netzwerks und arbeitet mit verschiedensten Akteuren aus Wissenschaft, Wirtschaft, Zivilgesellschaft und Verwaltung zusammen.

Web: <http://okfn.at>

10.2 Regierungsnahe Organisationen / Vereine

10.2.1 Werdedigital.at



WerdeDigital.at bündelt alle Informationen zum Thema „digitale Medienkompetenz.“ WerdeDigital.at stellt Wissensangebote, Qualifizierungsangebote und eine Serviceplattform für alle Lernangebote in Österreich zum Thema „digitale Medienkompetenz“ zur Verfügung. Die

Webseite richtet sich an alle Bevölkerungsgruppen

Institut zur Förderung digitaler Mediennutzung

Web: <https://www.werdedigital.at>

Vorstand: Mag.^a Meral Akin-Hecke, Mag. David Röthler, Mag. Alexander Uitz

10.2.2 Saferinternet.at



Saferinternet.at unterstützt vor allem Kinder, Jugendliche, Eltern und Lehrende beim sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien.

Die Initiative wird im Auftrag der Europäischen Kommission im Rahmen des CEF Telecom-Programms umgesetzt.

Saferinternet.at bildet gemeinsam mit der Stopline (Meldestelle gegen Kinderpornografie und nationalsozialistische Wiederbetätigung) und 147 Rat auf Draht (Telefonhilfe für Kinder, Jugendliche und deren Bezugspersonen) das „Safer Internet Centre Austria“. Es ist der österreichische Partner im Safer Internet Netzwerk der EU (Insafe).

Österreichisches Institut für angewandte Telekommunikation (ÖIAT)

Web: <https://www.saferinternet.at>

Vorstand: DI Barbara Buchegger, Jürgen Gangoly, DI Ronald Hechenberger, Erwin Rennert, Edward Strasser

10.3 Wirtschaftsnahe Organisationen & Vereine

10.3.1 ISPA Internet Service Providers Austria (ISPA)



Die ISPA ist die freiwillige Interessensvertretung von mehr als 200 Internet Service & Content Providern in Österreich.

Web: <https://www.ispa.at/>

10.3.2 Verein für Anti Piraterie der Film und Videobranche (VAP)



Seit seiner Gründung 2003 setzt sich der "Verein für Anti-Piraterie der Film- und Videobranche (VAP)" engagiert für die Rechte von österreichischen Filmverleihern, Home-Entertainment-Unternehmen, Film- und Fernsehproduzenten, Zulieferer der Filmbranche und Kreativen ein. Der VAP versucht, die Filmpiraterie in Österreich im Wesentlichen auf drei Wegen einzudämmen. Einerseits wird durch Öffentlichkeitsarbeit und Werbung das Unrechtsbewusstsein der Konsumenten gefördert, andererseits wird kommerzielle Film-Piraterie, insbesondere in Form der Server- und Internetpiraterie und in Form des Hard-Good Selling auf Flohmärkten, usw gerichtlich verfolgt, und drittens wird durch Lobbying-Arbeit auf regionaler, nationaler und internationaler Ebene angestrebt, den Stellenwert von geistigem Eigentum bei den Politikern und Behörden anzuheben.

10.3.3 Verband Alternativer Telekom Netzbetreiber



Der VAT, ein Netzwerkpartner des Fachverbandes der Elektro- und Elektronikindustrie (FEEI), wurde 1997 gegründet und ist die Interessenvertretung der im Zuge der Telekom-Liberalisierung neu in den Markt eingetretenen Betreiber.

Der VAT versteht sich als umfassende Interessenvertretung dieser Branche. Bei der Schaffung notwendiger und fairer Rahmenbedingungen kommt dem VAT gegenüber den Regulierungsstellen und Behörden auf österreichischer und internationaler Ebene - und gegenüber dem bisherigen Monopolisten - große Bedeutung zu.

Web: <http://www.vat.at/>

10.3.4 Verband Österreichischer Zeitungen (VÖZ)



Der VÖZ ist ein freiwilliger Zusammenschluss von Tageszeitungen, Wochenzeitungen und Magazinen. Er wurde 1946 gegründet. Als Interessenvertretung im klassischen Sinn befasst er sich – gemäß seinem Leitbild – mit allen Themenbereichen, die für die Verlage von zentraler Relevanz sind, wie z. B. Medienpolitik und -recht, Marketing, Vertrieb, Regelung von Arbeitsbedingungen für Mitarbeiter, Aus- und Weiterbildung etc.

Web: <http://www.voez.at/>

10.4 Europäische Organisationen

10.4.1 European Digital Rights



European Digital Rights is an association of [civil and human rights organisations](#) from across Europe.

Founded in June 2002, the Brussels office re-opened in 2009 and has expanded from one to four employees over the past two years.

Web: <https://edri.org>

President: Andreas Krisch

3

3D Druck · 24

A

Abwehrrechte · 46
AK Vorrat · 49
AKM · 59
AKVorrat · 82
Alan Rusbridger · 47
Alibaba · 10
Amazon · 58
APIS · 51
Austro Mechana · 59
Auto · 34
Autor · 55

B

B2B · 27
B2C · 27
Back Doors · 49
Big Data · 26, 35
Bildungssystem · 44
Bitcoin · 28
BitCoin · 33
Briefgeheimnis · 46
Bring your Own Device · 14
BVT · 54

C

CISCO · 75
Cloud · 31
Cloud Computing · 22
ClubComputer · 45
Cyberattacken · 75

D

Datenschutz · 25, 26, 35
Datenschutzbehörde · 62
Demonstrationsfreiheit · 46
Department of Homeland Security · 51
Deutsche Telekom · 80
Double Irish with a Dutch Sandwich · 27
Drei · 81

E

E-Call · 66
E-Democracy · 69
Edward Snowden · 10, 46, 47
E-Government · 70
ELGA · 63, 70
E-Mail · 42
Erwachsenenbildung · 45
Europe vs. Facebook · 62
Exekutive · 68

F

Fabrikarbeiter · 44
Facebook · 30, 31
Familie · 29
FCC · 80
Festplattenabgabe · 59
Finanz Online · 70
FISC · 23
FLAF · 42
Förderung · 39
Foreign Intelligence Surveillance Court · 23
Forschung und Entwicklung · 39
Forschungseinrichtungen · 73
Fotoapparat · 31
Fotograf · 55

G

Gamification · 42
Gebietsschutz · 57
Geheimdienste · 49
Gemalto · 75
George Land · 43
Gesundheitsdaten · 63
GIS · 74
Grünbuch · 7
Grundgebührenbefreiung · 74
Grundrechte · 46
Guardian · 47

H

Hausautomatisierung · 25

I

IMSI Catcher · 47
Indien · 80

Industriespionage · 75
Infrastruktur · 73
 Interessensvertretungen · 68
 Internet · 73
 Internet of Things · 25
 Internet Provider · 56
 internet.org · 80
 Internet.Org · 80
 IoT · 25
 ISPA · 85
 iTunes · 57

J

Judikatur · 68

K

Kommunikationsgeheimnis · 46

L

Legislative · 68
 Leistungsschutzrecht · 32
 Liquid Democracy · 69
 Literar-Mechana · 59

M

Massenüberwachung · 63
 Max Schrems · 62, 63
 Medienkompetenz · 41
 Meinungsfreiheit · 46, 47
 Metadaten · 49
Militär · 73

N

Navigationssystem · 34
 Netflix · 31, 78
 Netz · 76
 Netzneutralität · 80
 NFC · 33
 Nutzungsrecht · 31

O

OCG · 82
 Open Data · 71
 Open Educational Ressources · 42
 Österreichische Computer Gesellschaft · 82
 ÖVP · 80

P

Passagierdaten · *Siehe* PNR
 Passenger Name Record · *Siehe* PNR
 Patientendaten · 64
 Paul Rübig · 80
 PayPal · 28, 33
 Paywall · 32
 PCC-TGM · 41
 PNR · 63
 politische Parteien · 68
 Post · 26
 Pressefreiheit · 47
 Privatkopie · 58
 Privatleben · 29
 Privatsphäre · 46

R

Rakuten · 10
 Rechteinhaber · 58
 Reisefreiheit · 46
 Richter · 54

S

Safe Harbour · 63
 Schauspieler · 55
 Sicherheit · 25, 73, 74
 Skype · 30
 Smartmeter · 67
 SnapChat · 41
 Sofortüberweisung · 28
 Speichermedienabgabe · 59
 Spezialdienste · 79
 Spotify · 81
 Staatsschutzgesetz · 54
 Steuergesetzgebung · 27
 Streaming · 57



Stromzähler · 67
Stuxnet · 75

T

Telebanking · 33
Telekommunikationsgesetz · 49
Terror · 50
TVThek · 31

U

Urheberrecht · 31, 41, 42, 58
USA · 51

V

Verein für Anti-Piraterie · 86
Verfassungsgerichtshof · 49
Versammlungsfreiheit · 46

Versicherung · 26
Verwaltungstransparenz · 68
VG-Rundfunk · 59
VIBE.AT · 82
Vorratsdatenspeicherung · 49

W

WhatsApp · 30

Y

YouTube · 78

Z

Zahlungsverkehr · 28
Zero-Rating · 81
Zune · 57

11 Staatliche Stellen (EU / Österreich / Länder / Gemeinden)

Sozialministerium

<http://www.sozialministerium.at/site/Soziales/>

Bundesministerium für Familie & Jugend

<http://www.bmfj.gv.at/>

Gemeinde Wien – MA13 Bildung & außerschulische Jugendbetreuung

<https://www.wien.gv.at/freizeit/bildungjugend/>

Agentur der Europäischen Union für Grundrechte

<http://fra.europa.eu/de>

Portal Erwachsenenbildung des BMBF

<http://erwachsenenbildung.at>