DIGITALE NUTZERRECHTE

SCHWERPUNKT DATENSCHUTZ

AK WIEN

August 2014

GERECHTIGKEIT MUSS SEIN

ISBN Wien, August 2014
Wien, August 2014

AK Wien, Abteilung Konsumentenschutz
Prinz-Eugen-Straße 20-22
A-1040 Wien
Tel: ++43-1-501 65/3136 DW
E-Mail: konsumentenpolitik@akwien.at

DIGITALE NUTZERRECHTE

SCHWERPUNKT DATENSCHUTZ

Daniela Zimmer

Inhaltsverzeichnis

1. Kurzfassung Forderungen

Digitale Nutzerrechte
Schwerpunkt Datenschutz

Digitalisierungstechnik allgemein, das Internet im Besonderen verändern die Grundlagen und Spielregeln ganzer Lebensbereiche und Branchen. Neue Technologien und Dienstformen dringen tief in unseren Arbeits- und Konsumalltag, unser soziales Leben und Freizeitverhalten ein. Technologieschübe kosten Arbeitsplätze und bringen neue hervor. Wir sind privat wie beruflich mit den angenehmen wie unerwünschten Begleiterscheinungen der digitalen Entwicklung und des Lebens in einer Informationsgesellschaft konfrontiert. Bis zu einem bestimmten Grad haben wir uns mit Grauzonen und Regelbrüchen im Internet abgefunden. Das darf aber unser Engagement nicht bremsen, allen Schwierigkeiten zum Trotz auch für die digitale Welt nach wirksamen Konzepten der Rechtssetzung und Rechtsdurchsetzung zu suchen. Ohne Anspruch auf Vollständigkeit zählen jedenfalls zu den wichtigsten Zielen:

- **A-Priorität:** Politik setzt sich mit den uns umgebenden Technologien und ihren Auswirkungen auf die Gesellschaft ambitioniert auseinander. Die Herausforderung, auch im digitalen Zeitalter fundamentale Rechte wie jene auf Privatsphäre, den Datenschutz und die Informationsfreiheit, aber auch den allgemeinen Schutz digitaler NutzerInnen vor Übervorteilung zu gewährleisten, wird aktiver angenommen. Der Gesetzgeber, Regulierungs- und Vollzugsbehörden greifen schützend bzw korrigierend ein, wenn Kräfteungleichgewichte und Gefahren entstehen, die digitale Nutzerrechte unterminieren. Politik verschafft sich zeitgemäßes Wissen, um Trends frühzeitig zu erkennen. Internetregulierung bzw das Handlungsfeld der Technikgestaltung wird nicht allein Unternehmen und ihren Technikern überlassen. Damit Politik die Frage nach den Profiteuren der digitalen Revolution mit „wir alle“ beantworten kann, bekommen digitale Nutzerrechte allgemein und der Datenschutz im Besonderen einen hohen Stellenwert in der österreichischen und europäischen Politik. Sie werden quasi „Chefsache“.

- **Kompetenzzentrum:** Viele Gefahrenszenarien sind für die rechtspolitische Arbeit gut aufgearbeitet. Insoweit ist eine politische Priorisierung nötig, diese Themenfelder zielstrebig und nutzerfreundlich zu bearbeiten. Mit der Einrichtung eines Kompetenzzentrums für netzpolitische Studien bekommen Regierung, Parlament, Interessenvertretungen usw. Unterstützung bei der Bewertung und Entwicklung von Handlungskonzepten in Bezug auf digitale Märkte, Arbeits- und Lebenswelten.

- **Verbraucherschutz zur Freiheitssicherung:** Das in der EU-Grundrechtscharta verankerte Recht auf Schutz persönlicher Daten und der Privatsphäre erhält endlich den Stellenwert, der ihm in einer Gesellschaft gebührt, die auf Freiheitsrechten aufbaut. Das Selbstbestimmungsrecht jedes Einzelnen über die Nutzung seiner personenbezogenen Daten wird gegen wirtschaftlich und auch ordnungspolitisch motivierte Einschränkungen verteidigt und zeitgemäß ausgebaut. Verbraucherschutz bemüht sich auch um die Absicherung grundlegender Freiheiten.

- **Transparenz:** Datenverarbeitungsvorgänge, die häufig abseits der Wahrnehmung der davon Betroffenen stattfinden, müssen transparenter werden. Transparenz braucht es auch in anderen Zusammenhängen: bspw in Bezug auf die Kriterien der Reihung von Suchmaschinenergebnissen, bei Bewertungsplattformen, bei denen unklar ist, ob Produktempfehlungen manipuliert wurden oder Internetinhalten, die mangels Kennzeichnung redaktionellen Ursprungs sein können, aber auch simple Werbung.

- **Klarere Ge- und Verbote**: Die Rechtssicherheit in Bezug auf die Frage, ob eine bestimmte Datennutzung in unterschiedlichen Verwendungszusammenhängen der digitalen Welt zulässig oder unzulässig ist, wird verbessert**.** Dazu zählen klar umrissene Zulässigkeitsgrenzen für die Datenverarbeitung und Verarbeitungsverbote. Einzelfallsabwägungen bezüglich überwiegender Geheimhaltungs- oder Nutzungsinteressen an den jeweiligen Daten, die erst im Streitfall die Gerichte und Datenschutzbehörden vornehmen, sollten die Ausnahme sein.

- **Strikte Regeln für den Datenhandel statt Fiktionen von „freiwilligen" Zustimmungen:** Der digitale Datenhandel ist von Intransparenz und einem großen Kräfteungleichgewicht geprägt und bedarf einer rechtlichen Neuordnung. Die Zustimmung zur Datennutzung durch die Betroffenen ist vor diesem Hintergrund meist eine untaugliche Basis für die Zulässigkeit einer Datenverarbeitung. Der Schutz der Nutzer in Form gesetzlicher Beschränkungen für Datennutzungen wird deshalb intensiviert.

- **Unrechtsbewusstsein – Bewusstseinsbildung:** Bei vielen unberechtigten oder hinsichtlich von Datensicherheitsmaßnahmen nachlässigen Datennutzern muss Unrechtsbewusstsein erst geweckt werden. Die Datenschutzbehörde treibt daher über ihre Vollzugsaufgaben hinaus auch die Bewusstseinsbildung auf Seiten der Datenverwender voran. Auch eine effiziente Verwaltung bedient sich zur Politiksteuerung, Bedarfsplanung und Kontrolle zunehmend Auswertungen aus personenbezogenen Datenbanken. Der öffentliche Sektor misst sich in Datenschutzbelangen selbst an einem strengen Maß und geht ausnahmslos mit gutem Beispiel voran.

- **Datensparsamkeit:** Das Prinzip der Datensparsamkeit wird auf allen Ebenen forciert. Nicht alle Datennutzungen, die der Erreichung berechtigter Ziele dienen, sind auch durch ein überwiegendes Interesse legitimiert. Die Einholung einer Zustimmung bei den Betroffenen sollte nicht jeder Datennutzung die nötige Legitimität verschaffen. Denn typischerweise besteht ein erhebliches Kräfteungleichgewicht zwischen den Parteien. Von einer freiwilligen Zustimmung kann oft nicht die Rede sein. Andere Grundrechte wie jene auf Informations- und Eigentumsfreiheit sind zwar gleichermaßen zu beachten. Gerade der Grundsatz der Datensparsamkeit braucht aber eine Stärkung, soll er nicht völlig ins Hintertreffen geraten.

- **Vorbeugender Datenschutz** - bspw durch behördliche Vorabkontrollen oder die Forcierung des Erwerbs von Datenschutz-Gütezeichen - wird aufgewertet. Die nachträgliche Feststellung von Datenschutzverstößen und Schäden bietet keinen gleichwertigen Ersatz für deren vorsorgliche Verhinderung. Dazu zählt auch der vorbeugende Missbrauchsschutz durch möglichst konkrete sektorspezifische Datensicherheitspflichten. Bei der Datensicherheit darf auch dann nicht gespart werden, wenn sie im Einzelfall erhebliche Kosten verursacht.

- **Internetkonzerne auf dem Prüfstand:** Die Durchsetzung von Nutzerrechten gegenüber Internetkonzernen**,** die in Drittstaaten, vor allem den USA, niedergelassen sind, wird auf EU-Ebene intensiviert. Quasi-Monopole wie Google, Apple, Facebook, Amazon uä. verfügen über eine fast unbeschränkte Marktmacht, weltweite Präsenz und Kundendaten in gigantischem Umfang. Die EU-Kommission ist beharrlich daran zu erinnern, dass derartige „Over-the-Top-Player", die sich nicht an EU-Regeln gegenüber ihren europäischen Dienstnutzern halten, den Wettbewerb verzerren. Die Kommission hat Aufsichtsverfahren bzw informelle „Settlement"-Lösungen mit dem Ziel zu forcieren, dass globale Konzerne EU-konform verbraucher- und datenschutzrechtliche Verantwortung übernehmen.

- **Spürbare Sanktionen** bei systematischen Datenschutzverstößen. Derzeit müssen Datenverwender weder mit einer (raschen) Aufdeckung illegaler Datennutzungen noch mit abschreckenden Strafen rechnen. In der Regel wird erst aus Anlass massiver Beschwerden oder Medienberichten geprüft. Die Verhängung von (nennenswerten) Strafen ist absolut rar. Aufsicht und Sanktionen müssen an Wirksamkeit drastisch zulegen.

- **Leichter Zugang zum Recht**. Jedermann muss sich bei vermuteten Verstößen an eine Datenschutzbehörde wenden können, die möglichst niedrigschwellig Rat erteilt und Rechtsschutz gewährt. Die derzeitige Zersplitterung der Zuständigkeiten zwischen der Datenschutzbehörde und den Zivilgerichten ist überholt. Eine zeitgemäße Datenschutzbehörde muss demgegenüber einheitliche Anlaufstelle für Beschwerden über Verarbeitungen sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich sein.

- **Eine schlagkräftige Aufsichtsbehörde:** Ausstattung und technisches Knowhow der Datenschutzbehörde muss mit den hohen Anforderungen an ein solches Kontrollorgan Schritt halten. Angesichts millionenfacher Datenverarbeitungen braucht die Behörde Unterstützung, um einen Marktüberblick zu haben. Dazu zählen betriebliche Datenschutzbeauftragte in möglichst allen österreichischen Betrieben.

- **Staatliche Souveränität statt Spielball von Geheimdiensten:** Die Enthüllungen des ehemaligen US-Geheimdienstmitarbeiters Edward Snowden haben die exzessiven Spähaktivitäten der NSA und verbündeter Dienste ans Tageslicht gebracht. Es muss Konsequenzen geben. Die drängendsten Fragen über die Arbeitsmethoden von Geheimdiensten und des genauen Umfangs von geheimdienstlichen Datenschutzverstößen in Telekommunikationsnetzen sind rasch zu klären. Die parlamentarische Kontrolle von Geheimdiensten ist zu reformieren.

- **Rechtliche Konsequenzen aus der Geheimdienstaffäre:** Vordringlich sind strengere Standards für die Justiz- und Polizeizusammenarbeit und ihre analoge Anwendung auf Geheimdienste, mehr Rechtsschutzgarantien für die Betroffenen und Grenzen für Metadatenanalysen, mit denen aus großen Datenmengen – durch Filter, statistische Methoden usw. - auf Verhaltensmuster geschlossen wird. Betreiber von Exchange Servern sind datenschutzrechtlich stärker in die Pflicht zu nehmen. Telekomanbieter und Dienstleister, die den überregionalen Gesamtverkehr abwickeln, sollten verpflichtet werden, sich einem verpflichtenden Sicherheitsaudit zu unterwerfen.

- **Mehr Schutz vor Internetkriminalität:** Ob Fake-Shops, Phishing-Mails, Identitätsdiebstahl oder Hacking: Die Internetkriminalität in Österreich steigt. Nötig sind ressortübergreifende Schwerpunktaktionen, Schwerpunkt-Staatsanwaltschaften für den Cybercrime-Bereich, eine Präzisierung des Betrugstatbestands für das Onlineumfeld und eine Verbesserung der Strukturen für die grenzüberschreitende Zusammenarbeit, um das enorme Vollzugsdefizit (mehrheitliche Einstellung der Verfahren) zu verringern.

- **Digitale Spezialthemen regeln:** 1995 im Entstehungsjahr der Datenschutzrichtlinie gab es sie noch nicht oder nicht im gegenwärtigen Ausmaß. Gemeint sind Alltagsphänomene wie Always-on über (mobiles) Breitbandinternet, Big Data Analysen, Scoring und Profiling, digitale Marktforschung durch individuelles Tracking, verhaltensbasierte Onlinewerbung, Speichern in der Cloud, Cyber-Kriminalität, das „Mitmach"-Web 2.0, Netzkonflikte zwischen Informationsfreiheit und dem Datenschutz uvm. Themenspezifische Datenschutzregeln müssen daher die allgemeinen Grundsätze ergänzen. Damit werden die allgemeinen Vorgaben für das jeweilige Anwendungsfeld präzisiert.

- **Anonymisierungsgebot:** Anonymisierung als Ausdruck von Datensparsamkeit wird beim Vollzug des Datenschutzrechts forciert. Ist die Notwendigkeit eines Personenbezugs nicht eindeutig nachgewiesen, sind Daten vor ihrer Nutzung restlos zu anonymisieren. Pseudonymisierungen sollten die Ausnahme sein, da der Datennutzer den Personenbezug in diesem Fall wieder herstellen kann.

- **Höhere Anforderungen an die Zustimmung zur Datennutzung:** Zustimmungen durch stillschweigende Akzeptanz von (nicht gelesenen) Geschäftsbedingungen müssen der Vergangenheit angehören. Der Datennutzer muss sich jedenfalls um ein aktives ausdrückliches Zeichen der Betroffenen bemühen, also das Setzen eines Hakens beim Anklicken eines Kästchens im Internet oder Einholen der Unterschrift.

- **Mehr Schutz vor Direktmarketing:** Eine Privilegierung des Direktmarketings durch eine bloße Opt-Out-Regel (Widerrufsrecht) darf es nicht geben. Das Versprechen nach einem zeitgemäßen Datenschutz im Internet würde so nicht ansatzweise eingelöst werden. Verbraucher erwarten sich, dass ihre ausdrückliche Zustimmung zur Marketingnutzung ihrer Daten eingeholt wird (Opt In).

- **Datennutzung nur im Rahmen des Ursprungszweckes:** Daten dürfen nicht für Zwecke genutzt werden, die mit dem ursprünglichen Speicherzweck nicht in Einklang stehen. Ausnahmen von diesem Verbot (wie die Verarbeitung für statistische oder historische Zwecke) sind restriktiv zu handhaben und abschließend anzuführen.

- **Ausdehnung des EU-Datenschutzes auf Drittländer:** Es ist wichtig, dass die Anwendbarkeit der künftigen Datenschutz-Verordnung auf Drittländer wie bspw die USA ausgedehnt werden soll. Gleichzeitig müssen aber Vollstreckungsübereinkommen und Rechtsschutzhilfen vorangetrieben werden, andernfalls werden vorhandene Rechtsansprüche europäischer BürgerInnen weiterhin schwer durchsetzbar sein.

- **Automatische Verbraucherinformation:** Von Verarbeitungen Betroffene müssen vor der Datenermittlung mehr Informationen vom Datennutzer erhalten. KonsumentInnen müssen vorab unbedingt mitgeteilt werden: Namen und Kontaktdaten des Datenverantwortlichen, die Nutzungszwecke, die konkrete Speicherdauer, die Herkunft der Daten, ob die Bereitstellung der Daten verpflichtend oder freiwillig ist uä.

- **Strikte Auskunftspflicht über die Datenherkunft und Empfänger:** Die Auskunftspflicht bezüglich der Herkunft von Daten bezieht sich nur auf „verfügbare“ Daten. Datennutzer haben derzeit auch bloß über „Empfänger oder Empfängerkreise“ zu informieren. Der Verpflichtung wird schon entsprochen, wenn die Branche (zB „Finanzdienstleister“) offengelegt wird. Das jeweilige Unternehmen ist künftig zu benennen, damit der Betroffene seine Rechte überhaupt ausüben kann.

- **Spezielle Löschungsrechte im Internet:** Facebooknutzer veröffentlichen massenhaft Personendaten über sich und Dritte. Es bedarf daher eines Rechtsanspruchs auf vollständige Löschung selbstgenerierter Inhalte im Internet. Ein Fortschritt wäre auch die Verpflichtung desjenigen, der personenbezogene Daten im Internet veröffentlicht hat, Dritte, die diese Daten weiterverarbeiten, soweit als möglich darüber zu informieren, dass der Internetnutzer die Löschung aller Querverweise und Kopien verlangt hat.

- **Klare Grenzen für Profilbildung und Personenbewertung:** Die Vorschläge von EU-Kommission, EU-Parlament und Rat schaffen einen breiten Erlaubnistatbestand für die an Profiling interessierte Wirtschaft. Datenschutz und Rechtsschutzanliegen der Verbraucher kommen dabei zu kurz. Entscheidende Fragen werden ausgeklammert: unter welchen Voraussetzungen dürfen Personenprofile überhaupt gebildet werden? Welche Datenarten dürfen maximal verarbeitet werden?

- **Stopp für rechtswidrige Tracking-Methoden:** Die Regulierung des Einsatzes von technischen Werkzeugen, mit deren Hilfe das Nutzerverhalten im Netz nachverfolgt werden kann, muss wirksam und praxisnah sein. Die Anstrengungen zur Eindämmung des rechtswidrigen Ausspionierens des Surfverhaltens sind zu vergrößern. ZB braucht der Einsatz von Deep Package Inspection, einem Verfahren mit dem Datenpakete im Internet überwacht und gefiltert werden, restriktive Regeln.

- **Grenzen für die Nutzung von Big Data Analysen und Prognosen:** Gearbeitet wird mit Klassifikationen (zB Zuordnen zu Kreditwürdigkeitsklassen), Clustern (bspw die Definition einer Kundengruppe mit Neigung zum Anbieterwechsel) und Prognosen (zukunftsgerichtete Verhaltensannahmen). Datenanalysen werden bspw angestellt, um unerwünschte Kundenbeziehungen auszusondern. Es besteht Handlungsbedarf. Auch im Bereich datenbasierter Prognostik müssen geltende Datenschutzregeln wirksam durchgesetzt werden. Herkömmlicher Datenschutz ist um ein Verbot der Diskriminierung durch Bewertungsprozesse zu ergänzen. Rechtslücken sind in Bezug auf die Zweckbindung der Datenverarbeitung zu schließen.

- **Ausübungsregeln fürs Scoring:** Bonitätsbewertungen durch weitgehend automatisierte Scorings entscheiden immer öfter, ob KonsumentInnen als Vertragspartner akzeptiert werden. Klar ist, dass eine Kreditvergabe nicht ohne Überprüfungen ablaufen kann. Das Ausmaß der Regulierung ist derzeit aber dürftig. Es braucht rasch ein Scoring-Gesetz mit Ausübungsregeln, die unverhältnismäßigem Scoring Grenzen setzen. Betroffene dürfen zB keinen willkürlichen und diskriminierenden Verhaltenszuschreibungen ausgesetzt sein.

- **Mehr Eigenverantwortung der Datenverarbeiter:** Die EU-Kommission möchte Datennutzer stärker in die Verantwortung nehmen – durch verpflichtende Dokumentationen, Sicherheitsmaßnahmen, Datenschutzbeauftragte und eine Risikoabschätzung bei heiklen Datenanwendungen. Behördenaufgaben werden damit zwar „privatisiert". Klar ist aber auch: Datenschutzbehörden können nicht Millionen Datenanwendungen gleichzeitig im Auge behalten. Datenverarbeiter sollen sensible Vorhaben (die die Datenschutzbehörde bestimmt) durch unabhängige Kontrollstellen auf eigene Kosten prüfen lassen, damit Datenschutzkonformität gewährleistet ist und die Ergebnisse der Datenschutzbehörde vorlegen.

- **Melderegister beibehalten:** Das Melderegister erfüllt einen wichtigen Publizitätszweck (jedermann kann Einsicht nehmen) und gewährt der Datenschutzbehörde Einblick in die Verarbeitungspraxis. Unterlassene Meldungen sind für Datennutzer spürbar zu sanktionieren.

- **Privacy by Design und Default:** Datenschutz ist schon bei der Entwicklung neuer Technologien miteinzuplanen. Der diesbezügliche EU-Kommissionsvorschlag bleibt aber zu unverbindlich, um in der Praxis Nutzen zu stiften. Es braucht konkrete Vorgaben. Möglichst strenge Privatsphäre-Einstellungen bei Onlinediensten sind zB verbindlich vorzuschreiben.

- **Verpflichtende betriebliche Datenschutzbeauftragte:** Die verpflichtende Einführung eines betrieblichen Datenschutzbeauftragten in der Privatwirtschaft ist Kernstück jeder ernstzunehmenden Datenschutzreform. Der freie Datenfluss innerhalb der EU legt eine EU-weit einheitliche Regelung nahe. Vorschläge, Beauftragte nur in Unternehmen mit mehr als 250 MitarbeiterInnen vorzusehen (EU-Kommission) oder ab 5000 von der Datennutzung Betroffenen (EU-Parlament), gehen am Schutzbedürfnis des Einzelnen vorbei. Ziel ist eine obligatorische Einsetzung eines Beauftragten in möglichst vielen Unternehmen (bspw mit mehr als 20 MitarbeiterInnen).

- **Verbesserung des Datenschutzes für ArbeitnehmerInnen:** Es gibt kaum spezifische Vorschriften, die auf das besondere Schutzbedürfnis der Beschäftigten im Arbeitsverhältnis Bedacht nehmen. Ein Arbeitnehmer-Datenschutzgesetz wird deshalb in Angriff genommen. EU-Datenschutzregeln dürfen nationale Arbeitsverfassungen nicht berühren, also weder ihre Gültigkeit beschränken noch Betriebsratsrechte beschneiden. Arbeiterkammern und Gewerkschaften sollen zu den in Datenschutzangelegenheiten (verbands-)klagsberechtigten Einrichtungen gehören. Die Zulässigkeit von Datenübermittlungen sollte auf den Abschluss von Betriebsvereinbarungen abstellen. Konzerndatenschutzbeauftragte nur am Ort der Hauptniederlassung wären zu wenig: Beauftragte in Tochterunternehmen sollen Ansprechpartner vor Ort sein.

- **Verpflichtende Datenschutz-TÜVs:** Softe Förderung von Datenschutz-Gütezeichen greift zu kurz. In Bezug auf heikle Datenanwendungen muss Zertifizierung ein verpflichtender Standard sein. Ohne diesen Schritt werden die Datenschutzregeln den Ansprüchen des 21. Jahrhundert nicht gerecht.

- **Ausnahmslose Pflicht zur Meldung schwerwiegender Datenpannen:** Eine lückenlose Meldepflicht sollte selbstverständlich sein, um der Datenschutzbehörde die rasche Einleitung eines amtswegigen Prüfverfahrens zu ermöglichen und Betroffene solcherart vor weitergehenden Schäden zu bewahren.

- **Behördenzuständigkeit ohne One-Stop-Shop:** Das Konzept der EU-Kommission einer ausschließlichen Zuständigkeit der Datenschutzbehörde am Ort der Hauptniederlassung würde den Zugang zum Recht für Betroffene massiv erschweren. Konzerne werden animiert, sich an Orten mit besonders schwachem Datenschutzvollzug niederzulassen. Nationale Datenschutzbehörden sollten daher bei konzernweiten Datenverwendungen Betroffenen nicht nur als erste Anlaufstelle dienen, sondern auch entscheidungsbefugt sein.

- **Datenschutzbehörde als „Consultant“:** Abseits förmlicher Behördenentscheidungen ist der Dialog zwischen Datenverarbeitern und ihrer Aufsichtsbehörde zu intensivieren. Die niedrigschwellige Einholung von Expertise ist in einer von Kleinunternehmen geprägten Wirtschaft wichtig, sollen viele Datenschutzvorschriften nicht auch aus Unwissenheit und Überforderung unbeachtet bleiben.

- **Wirksame Rechtsdurchsetzung:** Nötig ist eine Risikominimierung heikler Datennutzungen durch behördliche Vorabkontrollen. Neben dem Vertretungsrecht in datenschutzrechtlichen Verfahren sollte Einrichtungen, die die Interessen von ArbeitnehmerInnen und VerbraucherInnen wahrnehmen, eine Verbandsklagsbefugnis zukommen.

- **Regelbrüche und Vollzugsdefizite:** Regelbrüche im Netz überfordern zum Teil den Rechtsstaat. Staatliche Kontrollorgane, Daten- und Verbraucherschützer können der Vielzahl verfolgenswerter Handlungen im Internet wenig entgegensetzen. Ausstattung und Arbeitsweise von Behörden und Justiz entsprechen nicht den Anforderungen des digitalen Zeitalters und sind daher massiv auszubauen. Ziel ist, dass Ermittlungen auch in kleindimensionierten (zB Streuschäden mit vielen Betroffenen) und besonders großdimensionierten (zB Internetkonzerne, Geheimdienste) Fällen durchgeführt werden.

- **Stärkung der Datenschutzbehörde:** Wegweiser in die Zukunft muss eine gut ausgestattete Datenschutzbehörde sein, die ihre Ratgeberfunktion ausbaut, öffentlichkeitswirksam Datenschutzbewusstsein schafft, Missstände aufzeigt und als Kompetenzzentrum zur Weiterentwicklung des Datenschutzes dient. Die Zuständigkeiten der Datenschutzbehörde sind überholt und werden deshalb neu geordnet. Statt einer zivilgerichtlichen Zuständigkeit mit Anwaltszwang sollen Betroffene ihre Datenschutzansprüche gegenüber der Privatwirtschaft auch bei der Datenschutzbehörde durchsetzen können.

- **Abschreckende Verwaltungsstrafen:** Abschreckende Strafdrohungen sind wichtig. Sie müssen allerdings auch vollzogen werden. Wird die Strafgewalt bspw wegen der Unterfinanzierung der Behörden kaum angewendet, so bleibt die Wirkung einer – wenn auch hohen – Strafdrohung in der Praxis gering.

- **Einbeziehung von Stakeholdern in die Behördenarbeit:** Bis 2014 wurden Aufsichtsfunktionen und (neben den Zivilgerichten) ein Teil des Rechtsschutzes von der im Bundeskanzleramt eingerichteten Datenschutzkommission als Kollegialorgan (unter richterlichem Vorsitz und unter Einbindung von Mitgliedern, die von den Ländern, der AK und WKÖ nominiert wurden) wahrgenommen. Nun ist die Behörde monokratisch (Leiter und Stellvertreter).

Durch Aufgabe der Einbindung von Stakeholdern mit unterschiedlichem Wissens- und Erfahrungshintergrund ist ein wichtiges Element deliberativer Entscheidungsfindung verloren gegangen. Ihre angemessene Teilhabe an den vielen Wertungsentscheidungen der Behördenpraxis ist wieder sicherzustellen.

- **Zusammenwirken von nationalen und EU-Institutionen:** Ein gemeinsames Auftreten von Datenschutzbehörden, der EU-Kommission und Verbraucherverbänden schafft jene Verhandlungsmacht, die nötig ist, um die Marktbearbeitungspraktiken weltweit agierender Internetkonzerne zugunsten der Rechte und Bedürfnisse digitaler NutzerInnen zu beeinflussen. Dieses Zusammenwirken ist zu institutionalisieren. Vergleiche dürfen die Mitgliedstaaten allerdings nicht daran hindern, einzelne Rechtsfragen auf dem Rechtsweg zu klären.

- **Erleichterungen für Konsumentenorganisationen:** Unterlassungsurteile in einem Land hindern Anbieter nicht daran, aufgrund der territorialen Wirkung von Entscheidungen anderswo auf dieselbe unseriöse Geschäftspraxis zu setzen. Zu überdenken ist, inwieweit Parallelentscheidungen in anderen Mitgliedstaaten verfahrensökonomisch erleichtert werden können. Ein EU-weites Firmenbuch und eine Reform der Verbindungsstellen nach der E-Commerce-Richtlinie sind überfällig.

- **Datenübermittlungen außerhalb der EU:** Die USA ist im Datenaustausch mit Europa wichtigste Datenempfängerin und begeht zugleich nachweislich systematische Datenschutzverletzungen. Angesichts des in der Praxis als wertlos geltenden „Safe Harbour-Abkommens“ zwischen EU und der USA führt kein Weg daran vorbei, Datentransfers in Länder, die über kein gleichwertiges Datenschutzniveau verfügen, zu beschränken.

- **TTIP - Priorität für strikten Datenschutz:** Im Zuge der TTIP-Verhandlungen über ein Freihandelsabkommen zwischen den USA und der EU darf die EU den Konflikt zwischen verschiedenen Datenschutztraditionen nicht scheuen. Sie hat sicherzustellen, dass die EU-Datenschutzregeln nicht ausgehöhlt werden und weiterentwickelt werden können.

- **Wunschsperren für automatische Suchmaschinenzugriffe auf Websites mit Augenmaß**: Der Europäische Gerichtshof hat Google 2014 verpflichtet, Suchergebnisse auf Wunsch eines Betroffenen zu löschen. Mit dieser Wertung handelte sich der EUGH bei Kritikern den Vorwurf ein, Zensur zu begünstigen. Auf EU-Ebene sind u.a. die Kriterien für die Durchführung bzw Verweigerung einer Löschung zu klären.

- **Transparente und faire Suchmaschinenrankings:** Google mit über 1 Milliarde monatlichen Besuchern bemüht sich um den Eindruck, die Ergebnisreihung käme mit Hilfe unbestechlicher Suchalgorithmen zustande. Die Faktoren, nach denen eine Website von Suchmaschinen transparent und wettbewerbsneutral gereiht wird, sind breit zu diskutieren. Techniken, die über eine Suchmaschinenoptimierung hinausgehen und Reihungsergebnisse manipulieren, müssen aktiver zurückgedrängt werden.

- **Datenschutzvorgaben für die Nutzung von Sozialen Netzwerken:** Betreiber sind mit Nachdruck aufzufordern, Einstellungen zum Schutz der Privatsphäre anzubieten, diese strikt voreinzustellen und Datenschutz-Bestimmungen verlässlich einzuhalten. Die meisten Plattformen finanzieren sich über zielgerichtete Werbung.

Dieses Geschäftsmodell lässt sich mit der Idee der Datensparsamkeit schwer in Einklang bringen. Durchzusetzen ist zumindest, dass u.a. Datenfreigaben von den Nutzern eigens angehakt und Nutzerdaten nach Widerruf von freiwilligen Zustimmungen bzw der Beendigung der Dienstnutzung vollständig physisch gelöscht werden. Im Missbrauchsfall (zB Identitätsdiebstahl) muss der Betreiber auf Sperrmeldungen rasch reagieren.

- **Datenschutzregeln für geobasierte Dienste:** Smartphone-NutzerInnen sind identifizierbar über UDID/IMEI, Telefonnummer, Zeit-Weg-Profile, diverse Login-Daten uvm. NutzerInnen benötigen mehr Schutz vor der Analyse und Ausbeutung ihrer Geodaten (Standort, Bewegungstempo uä.) durch restriktive gesetzliche Regeln. Überwachungsphantasien neuer Dimension (etwa des Fahrverhaltens von PKW-Lenkern durch KFZ-Versicherungen) ist eine Absage zu erteilen. Der Zugriff auf Geodaten ist durch Piktogramme am Display leicht erkennbar zu machen. Benötigt werden außerdem feiner abgestufte Einwilligungen zum Datenzugriff.

- **Mindestharmonisierung für weitere datenschutzsensible Sektoren oder Techniken:** Fast jede technische Anwendung zieht dringliche Fragen und Bedenken hinsichtlich der Vertraulichkeit und der Sicherheit von Daten nach sich, wenn sie zur Sammlung persönlicher Daten genutzt werden kann. Die abstrakten Datenschutz- und Sicherheitsregeln sind zu präzisieren zB beim Einsatz der Funkfrequenzkennzeichnung (RFID), Biometrie, elektronischen Geldbörsen, computerdominierten Autos (Connected Cars), intelligenten Zähler (Smart Meter) und datenschutzsensibler, öffentlicher digitaler Anwendungen.

- **Onlinewerbung:** Zu den elementaren Prinzipien der Werbung zählt: Sie muss klar als solche erkennbar sein. Sie darf das Recht auf Privatsphäre nicht verletzen. Sie darf keinen (in-) direkten Kaufzwang auf Minderjährige ausüben. Diese Prinzipien haben im Internet wenig Gewicht. Mit werblichen Belohnungssystemen in Spielen, Werbung in Apps und In-App-Käufen werden KonsumentInnen oft in die Irre und in Kostenfallen geführt. Der Vollzug geltenden Rechts muss verbessert werden, damit Werbung und Sponsoring auch in der digitalen Welt transparent sind, Kinder nicht überrumpelt und keine rechtswidrigen Verhaltensprofile angelegt werden.

- **Faire Nutzerrechte in Bezug auf urheberrechtlich geschützte digitale Güter:** Anpassungen des Urheberrechts an die digitale Welt dienen vorrangig der Position der RechteinhaberInnen. Dabei sind neue Abhängigkeiten entstanden: Was Nutzer mit erworbenen digitalen Inhalten anfangen können oder nicht, regeln Anbieter einseitig zu ihren Gunsten über technische Schranken und Lizenzbedingungen. Deshalb sind nun auch die Konsumentenrechte zu stärken**,** etwa durch konkret durchsetzbare freie Werknutzungsansprüche wie digitale Privatkopien, einen tatsächlich freien Binnenmarkt sowie spezifische Mindestvertragsinhalte für den Abruf digitaler Güter.

- **Rechtschutzgarantien bei der Durchsetzung geistiger Eigentumsrechte:** Einige Maßnahmen sind geeignet, die Privatsphäre und Informationsfreiheit der NutzerInnen zu beeinträchtigen. Außergerichtliche Eingriffe in die Nutzerrechte sollten nicht zulässig sein. Internetprovider können zB nicht selbst über Datenweitergaben, Filtermaßnahmen bzw Kundensperren entscheiden. Alle Grundrechtseingriffe gegenüber InternetnutzerInnen müssen deshalb einem Richtervorbehalt unterliegen.

InternetnutzerInnen brauchen zudem Schutz vor einer „Abmahnindustrie“, die private Internetnutzer wegen tatsächlicher oder vermeintlicher Rechtsverletzungen mit überhöhten Forderungen verfolgt.

- **Koordinierte Netzpolitik:** Ob Jugendschutz, Straf-, Urheber-, Konsumentenschutz- oder Medienrecht – Netzpolitik erweist sich als denkbar weite Querschnittsmaterie, die auch regierungsseits entsprechend intensiv zu koordinieren ist. Dazu werden Stakeholder, die Nutzerinteressen vertreten, intensiv in die rechtspolitische Arbeit eingebunden. Auch die institutionelle Zusammenarbeit verschiedener Ressorts und Behörden (Datenschutz- und Telekomregulierungsbehörde, BKA, BMI, BMASK, BMVIT uvm.) ist zur Bewältigung von Querschnitts-Problemen auszubauen.

- **Netzneutralität:** Auch die Sorge um den Bedeutungsverlust der “Netzneutralität“ zeigt, dass Laissez Faire keine Handlungsoption ist. Ziel ist ein gesetzlicher Rahmen, der einen Zerfall des Netzes in verschiedene Unterklassen abhängig von der Zahlungsfähigkeit der Diensteanbieter und Nutzer verhindert. Es braucht regulatorische Maßnahmen, die die Nutzererwartungen an einer (weitgehenden) Gleichbehandlung transportierter Datenpakete schützen und zwar in Hinblick auf Transparenz der erworbenen Dienstleistung, Achtung der Grundrechte, Angebotsvielfalt, Wahlfreiheit, Qualität der Dienste, Bekämpfung unfairen Wettbewerbs und der Förderung innovativer Dienste.

- **Marktkonzentration:** Globale Konzerne wie Google, Amazon und Facebook haben eine Marktmacht, der nationale Regierungen und EU-Einrichtungen zu wenig entgegensetzen. Prioritäres Ziel der EU-Kommission sollte es sein, durch (weitere) Aufsichtsverfahren fairen Wettbewerb im Internet durchzusetzen. Zwecks Innovationsförderung sind Open Source- bzw freie Software zu unterstützen, die auch Dritten Weiterentwicklungen ermöglicht.

- **Open Data:** Open Data steht für die Idee, (meist öffentliche) Daten allgemein verfügbar und nutzbar zu machen. Neben vielen positiven Aspekten einer Freigabe dieser Daten zur Weiterverarbeitung gibt es auch nicht wenige Bedenken an der uferlosen Verwertbarkeit öffentlicher Daten, die unter Umständen nicht ausreichend anonymisiert sind. Fragen der Haftung, des Urheberrechtes usw. bedürfen einer eingehenden Klärung.

- **Partizipationsverfahren bei Themen mit großen gesellschaftlichen Auswirkungen:** Ob private Videoüberwachung mit kostengünstigen Videokameras aus dem Baumarkt, elektronische Patientenakte oder digitale Stromzähler für alle Haushalte. Diese Trends berühren praktisch jeden. Es sollte öfter auf Partizipationsmodelle zurückgegriffen werden, über die betroffene BürgerInnen informationell gut eingebunden sind, Sorgen und Ängste Beachtung finden und unerwünschte Folgen bzw Alternativen gründlich erforscht werden.

- **Basisfinanzierung für die Betrugspräventionsarbeit:** Die Weiterführung der für InternetnutzerInnen wichtigen Aufklärungs- und Unterstützungsaktivitäten von Initiativen, wie der Watchlist-Internetbetrug, des Internetombudsmanns oder der Safer-Internet-Initiative ist längerfristig finanziell abzusichern.

- **Medienkompetenz und Risikobewusstsein** gegenüber Risken im Internet sind durch schulische und außerschulische Bildung und Aufklärung zu vermitteln. Auch betriebliche Datenschutzbeauftragte wären enorm wichtige Informationsdrehscheiben, die Wissen an MitarbeiterInnen weitergeben und kritische Diskussionen über risikobehaftete Technologien in ihrem Umfeld anstoßen könnten.

Langfassung

Digitale Nutzerrechte
Schwerpunkt Datenschutz

Frank Schirrmacher, Mitherausgeber der FAZ, *1959 -†2014, galt als Vordenker offener Fragen der digitalen Welt. Am deutschen Verbrauchertag 2013 (siehe Jahresbericht des VZBV) resümierte er treffsicher:
Verbraucherschutz in der Informationsökonomie wird zu einer politisch hochbedeutsamen Aufgabe. Er muss sich – will er mit der neuen Welt mithalten – zu einem Instrument von Freiheitssicherung entwickeln. Die Unantastbarkeit der Person zu gewährleisten, ist im digitalen Zeitalter eine gänzlich neue Herausforderung. Eric Schmidt [Anm.:Google-Vorstand] schreibt, Persönlichkeit wird künftig der wertvollste Rohstoff der Bürger sein. Und Identität wird vorrangig online existieren. Online-Erfahrungen werden mit der Geburt beginnen – oder noch vor der Geburt, wenn sogar schon Ultraschallfotos ins Netz gestellt werden. Der Verbraucher im digitalen Zeitalter kauft nicht nur ein Produkt, er wird tatsächlich selbst zum Produkt. Er wird gelesen, wenn er kauft. Er wird gelesen, wenn er sich bewegt. Er wird gelesen, wenn er liest, wenn er bezahlt, sogar wenn er denkt…Im Zeitalter von Big Data wird potenziell alles zum Markt, auch die Politik und das soziale Leben.

2. Einleitung

Ausgangspunkt für das folgende Papier ist die Erkenntnis: Das in der EU-Grundrechtscharta verankerte Recht auf Schutz persönlicher Daten und der Privatsphäre erhält nicht (immer) jenen Stellenwert, der ihm in einer Gesellschaft gebührt, die auf Freiheitsrechten aufbaut. BürgerInnen verfolgen quer durch Europa, ob sie auch in sozial und wirtschaftlich schwierigen Zeiten darauf vertrauen können, dass die europäische Union und ihre Mitgliedstaaten historisch mühsam errungene fundamentale Rechte ernst nehmen. Dazu zählt das Selbstbestimmungsrecht jedes Einzelnen über die Nutzung seiner personenbezogenen Daten. Dieses scheint immer öfter auf der Kippe zu stehen. Der Schutz digitaler NutzerInnen erfordert ganz allgemein mehr Anstrengungen und zum Teil auch Lösungen, die über die (zivil-, verwaltungs- und strafrechtlichen) Instrumente des Analogzeitalters hinausgehen.

Alles bestens? Allen Mahnungen zum Trotz lassen wir uns gerne auf Risiken und Wagnisse im Internet ein. Wir schließen mit nicht näher bekannten Personen und Unternehmen Onlineverträge, erwerben Waren auf Basis bloßer Abbildungen, erzählen völlig Fremden in Foren unsere Sorgen und kommentieren ausgiebig politische Meldungen in Blogs und über Kommentarfunktionen von Internetseiten. Und trotz wachsenden Missbrauch der Privatsphäre und steigender Internetkriminalität: erstaunlich viele der auf Vertrauensvorschuss basierenden Internetaktivitäten zwischen Privatpersonen und Unternehmern, die einander zuvor nicht begegnet sind, wickeln wir ganz zufrieden ab. Privatwohnungen oder Mitfahrgelegenheiten werden online gebucht. Ungeheure Mengen an gebrauchten Sachen werden über Auktions- und Kleinanzeigenplattformen verkauft. Bürgerinitiativen werben für ihre Anliegen. Selbsthilfegruppen werden online ins Leben gerufen. Im Rahmen von wissenschaftlichen Internetprojekten tragen BürgerInnen Daten zusammen, die in dieser Menge von Forschern nicht bewältigt werden könnten.

Onlineaufrufe zum Crowdfunding ermöglichen Musikgruppen, Spielentwicklern uvm, Vorhaben zu verwirklichen, in dem sie online finanzielle Unterstützer suchen, die später das realisierte Werk erhalten. Dieser positive Befund ließe sich noch lange fortsetzen. Die vielen Vorzüge der leichten und kostengünstigen Erzeugung, Verbreitung und Weiternutzung von Inhalten im Internet dürfen aber nicht darüber hinwegtäuschen, dass wir vor einer ebenso langen Liste – gesellschaftlich und rechtspolitisch – ungelöster Probleme stehen.

Permanente Veränderungen: Es ist wissenschaftlich gut aufgearbeitet, wie die Digitalisierungstechnik und dabei vor allem das Internet die Grundlagen und Spielregeln ganzer Lebensbereiche und Branchen in den vergangenen Jahren verändert haben. Viele Wirtschaftsbereiche haben die Auswirkungen des Internets zu spüren bekommen. Ob Handel, Reisedienstleister oder Werbebranche: viele Anbieter ringen mit der temporeichen Abfolge digitaler Innovationen und letztlich damit, verdrängt zu werden oder sich den neuen Produktions- und Vertriebsformen anzupassen. Neue Technologien dringen in immer rascher aufeinander folgenden Zyklen tief in unseren Arbeitsalltag, unser soziales Leben und Freizeitverhalten ein. Sie überfordern oft ältere Menschen, begeistern junge und setzen Eltern und ihrem Erziehungsstil Belastungsproben aus. Sie verändern die Arbeitsweise im Rahmen des Berufs, der Bildung und Forschung. Technologieschübe beseitigen Arbeitsplätze und bringen neue hervor. Wir sind privat wie beruflich mit den angenehmen wie unerwünschten Begleiterscheinungen der Entwicklung der Digitaltechnik und des Lebens in einer Informationsgesellschaft konfrontiert. Chancen und Risiken liegen oft eng nebeneinander.

Das Anhäufen von personenbezogenen Daten im gegenwärtigen gigantischen Umfang wäre ohne die enorme Verbreitung neuer Informations- und Kommunikationstechnologien undenkbar. Rechenkapazitäten und Vernetzung erlauben es, Informationen mit einer noch nie dagewesenen Effizienz zu verarbeiten. Was früher Jahre gebraucht hat, ist inzwischen in Minuten möglich. Die verfügbaren Datenarten haben sich dabei vervielfacht, nicht zuletzt, weil sie in der Regel bereits in digitaler Form erzeugt werden. Mit der Gewohnheit des „Always On-“, des „Immer dabei“- Internets in Form von Smartphones, Beiträgen auf Facebook rund um die Uhr und PKWs, die zu fahrenden, vernetzten Computern hochgerüstet werden, fallen permanent digitale Daten an. Die leichte Verfügbarkeit erhöht selbstverständlich den Reiz, angehäuftes Datenmaterial nicht brachliegen zu lassen, sondern einer weiteren Verwertung zuzuführen - im Dienste kommerzieller Geschäftsideen, der staatlichen Verwaltungs-optimierung, medialer Berichterstattung, der Wissenschaft, der Kriminalprävention und Strafverfolgung, leichterer Rechtsdurchsetzung und, und, und….

Rohstoff „Daten“: Schon 2006 galt in der amerikanischen Werbebranche die Devise: “Daten sind das neue Öl”. Aktuell bestätigt sich die Treffsicherheit dieses Ausspruchs in vielen Wirtschaftssektoren aber auch im öffentlichen Bereich: Daten sind im Informationszeitalter ein wertvoller Rohstoff. Vergleichbar mit Öl, das zu unterschiedlichen Produkten verarbeitet wird, sind auch Daten das Material, das zu Datenanwendungen und Diensten „veredelt“ wird. Der Datenhandel erweist sich dabei generell als Geschäft, das von einem großen ökonomischen Ungleichgewicht und fehlender Transparenz geprägt ist. Die Rechtslage bietet zwar grundsätzlich Schutz vor überschießenden und den Einzelnen beeinträchtigenden Datenflüssen. Die Kontrolle der bestehenden Regelungen stellt sich aber zunehmend als schwierig oder geradezu aussichtslos dar. Hinzu kommt, dass das Unrechtsbewusstsein bei vielen unberechtigten Datennutzern gering ist.

Selbstbedienung im Internet: VerbraucherInnen, ArbeitnehmerInnen, schlicht jede/r BürgerIn spüren in seiner/ihrer Lebenswelt inzwischen das Primat wirtschaftlicher Verwertungsinteressen an persönlichen Daten recht deutlich. E-Mails, Onlinebanking und Einkaufen per Mausklick: niemand nimmt ernsthaft an, dass die bei solchen Aktivitäten anfallenden Informationen in einem verschlossenen Briefumschlag stecken, der vor jedem Blick geschützt ist. Der Druck, vorhandene Informationen zu verwerten, lastet nicht nur auf gewinnorientierten Unternehmen, sondern auch auf öffentlich-rechtlichen Institutionen: der vermeintliche Sicherheitszugewinn für die Gesellschaft durch wachsende Sammlung und Auswertung von personenbezogenen Daten setzt dabei häufig die Privatsphäre aufs Spiel. Auch eine effiziente Verwaltung mit ihren rigiden Zielvorgaben setzt zur Politiksteuerung, Bedarfsplanung und Kontrolle auf den Ausbau und die Verknüpfung von Datenbanken, die Personendaten enthalten.

Gemischte Bilanz: Das Internet hilft BürgerInnen, Anliegen vorzubringen und zu verbreiten. Gleichzeitig wird es als staatliches Überwachungswerkzeug derselben BürgerInnen missbraucht. Folgerichtig fragt die Initiative „European Digital Rights“: Nutzen Staaten die digitalen Errungenschaften, um ihrer Bevölkerung im Internet eigentlich zuzuhören oder sie abzuhören? Vermutlich hat das Internet unsere Informationslage gehörig verbessert. Unter Umständen verdrängt es aber längerfristig auch qualitativ hochwertige Berichterstattung, wie wir sie von herkömmlichen Medien kennen und schätzen. Das Internet hat uns zu zeitlicher und örtlicher Autonomie verholfen. Gleichzeitig tauchen neue soziale Abhängigkeiten auf. KonsumentInnen dürfen sich über einen Zugewinn an Bequemlichkeit freuen. Gleichzeitig bezahlen sie den Komfort doppelt - mit dem Kaufpreis und dem Zugriff auf ihre persönlichen Daten, aus denen oft nicht sie selbst, sondern Dritte Profit schlagen. Oft gibt es für KonsumentInnen keine brauchbaren Alternativen, bei denen nicht große Teile der Privatsphäre verloren gehen. Oft fehlen also schlicht Handlungsoptionen. Die kompromissloseste Lösung zugunsten des Datenschutzes ist, sich an der digitalen Entwicklung gar nicht zu beteiligen. Ein Rückzug aus der digitalen Welt bleibt natürlich für die meisten reine Theorie. Im beruflichen und privaten Leben wird Onlinepräsenz schlicht erwartet. Und grundsätzlich wollen wir auch nicht gerne vom gesellschaftlichen Leben ausgeschlossen sein.

Die Schattenseite: Elektronische Kommunikation und Informationssuche ist leicht und vielfältig wie nie zuvor. Wir durchschauen dabei aber in der Regel weder Geräte, Software noch Dienste weit genug, um behaupten zu können, unsere Alltagstechnik zu verstehen geschweige denn im Griff zu haben. Wir begreifen, dass eigentlich umgekehrt die Technik uns fest im Griff hat. Wenn bspw ohne aufgedrängte Softwareaktualisierung nichts mehr läuft oder Hersteller uns mit bewussten Unvereinbarkeiten zwischen Komponenten gängeln. Prozesse wie Profiteure sind für uns undurchsichtig. Die Fäden werden abseits unserer Wahrnehmung hinter den Kulissen der Benutzeroberfläche gezogen. Verstärkt wird dieser Ohnmachtseindruck noch durch Medienberichte über jahrelange Überwachungsexzesse europäischer und amerikanischer Geheimdienste. Aber auch Telekom- und Internetkonzerne scheinen immer wieder Gefahr zu laufen, als verlängerter Arm staatlicher Sicherheitsinteressen betrachtet zu werden. Die Unentbehrlichkeit von Google, Apple & Co im Alltag hat zur Folge, dass einige Konzerne über unsere Lebensgewohnheiten und Eigenschaften möglicherweise besser Bescheid wissen als wir selbst.

Kontroverse über Rechte im Internet: Aktuell ist ein rechtspolitisch heftiges Tauziehen zwischen den konträren Interessen an einer berechtigten Nutzung auf der einen bzw der Geheimhaltung von Informationen auf der anderen Seite zu beobachten. Das Gebot der Stunde für die EU- wie die nationale Politik ist ein umsichtiger, kompetenter Umgang mit unseren Freiheitsrechten. Politische Lippenbekenntnisse zugunsten des Schutzes der Grundrechte gibt es viele. Damit ist niemandem gedient.

Es braucht eine ernsthaftere, ehrgeizigere politische Hinwendung zu den offenen Fragen unserer digitalen NutzerInnenrechte und im Besonderen der Gefährdung unserer Daten. Denn die Frage, wem die bisherige digitale Entwicklung nun genau zu Gute kommt, wird durch die ungeheure Marktdominanz einiger Internetkonzerne, der Bedrohung unserer Privatsphäre, dem Erwerb bloßer Onlinenutzungsrechte statt physischer Güter uä. um viele Facetten reicher.

Mehr NutzerInnenrechte: Weiterentwickelte Online-NutzerInnenrechte, vor allem strikter Datenschutz, tragen dazu bei, dass von der digitalen Entwicklung nicht nur wenige, sondern möglichst alle profitieren. Der permanente Verstoß gegen die Grundsätze des europäischen Datenschutzes untergräbt auch die Wirksamkeit und gesellschaftliche Akzeptanz der missachteten Regeln. Das Einholen einer „Zustimmung zur Datennutzung in Kenntnis der Sachlage“ („informed consent“) gerät zum reinen Feigenblatt. Denn die Betroffenen werden meist nicht ausreichend informiert, haben oft nicht das erforderliche Knowhow, um die Tragweite ihrer Entscheidung zu erfassen, und sind noch viel öfter ohnehin alternativlos, weil ihnen ohne die abverlangte Zustimmung die Dienstnutzung einfach verwehrt bleibt. Mehr als alles andere ist es deshalb geboten, Datenschutzeinrichtungen mit Ressourcen auszustatten, damit sie ihrer Aufgabe nachkommen und dem bestehenden Recht zur Durchsetzung verhelfen können.

Die Ziele: Was wir nicht wollen ist: Datenschutz bzw digitale Nutzerrechte nur für eine Minderheit, die zu allen technischen Entwicklungen Abstand hält, sich eine kostspielige zivilrechtliche Abklärung bzw Rechtsdurchsetzung leisten kann oder kraft überdurchschnittlichen technischen Fachwissens sich selbst zu helfen versteht. Einfache Antworten auf die digitalen Herausforderungen gibt es natürlich selten. Viel wäre schon erreicht, wenn zumindest über die Ziele weithin Einigkeit herrschte. Auch davon sind wir noch weit entfernt. So sollte eigentlich Einvernehmen darüber bestehen, dass personenbezogene Daten im Internet nicht im Eigentum von Onlineanbietern und Werbewirtschaft stehen. Es geht auch nicht an, dass jeder denkmögliche Zusammenhang unterschiedlichster Daten aus unterschiedlichsten Quellen ermittelt und verwertet wird – sei es in Gewinnabsicht oder auch im (gutgemeinten) öffentlichen Interesse. Löschanliegen einzelner Betroffener ist im Internet unbedingt nachzukommen. Das gebieten Persönlichkeitsrechte und der Datenschutz. Die Grenze ist aber dort erreicht, wo wir auf berechtigte Kritik, Zensur zu üben, stoßen. Einwände zB von Journalisten und Historikern sind deshalb ebenso genau zu beachten. Bis zu einem bestimmten Grad haben wir uns mit den vielen Graubereichen und Rechtsverstößen im Internet einfach abgefunden. Das darf aber nicht unser Engagement bremsen, nach wirksamen Konzepten der Rechtssetzung und -durchsetzung zu suchen. Die größte Schwierigkeit ist dabei, dass, indem wir das Recht einer Person schützen, häufig zugleich in Rechte anderer Personen eingreifen. Jeder regulatorische Reflex erzeugt im Netz auch Gegenreflexe. Vollzugsmaßnahmen gegen Internetkriminalität lösen zB Umgehungstaktiken aus. Trotz aller Mühsal für den Rechtsstaat: bei der Wahl staatlicher Kontrollmittel darf nicht in Kauf genommen werden, dass die Grundrechte unbeteiligter Dritter erheblich beeinträchtigt werden.

Höchste Priorität: In jedem Fall wächst der Wunsch nach einer Politik, die sich mit den uns umgebenden Technologien ambitionierter auseinandersetzt und mehr Verständnis für ihre Auswirkungen auf die Gesellschaft aufbringt. "Das Internet ist für uns alle Neuland" – mit diesen Worten antwortete die deutsche Kanzlerin Angela Merkel 2013 bei einer Pressekonferenz auf eine Frage zum Internet-Spähprogramm Prism. Für dieses Bekenntnis erntete die Spitzenpolitikerin Spott. Auch die Politik muss mit zeitgemäßem Wissen ausgerüstet im digitalen Zeitalter ankommen und Internetregulierung und das Handlungsfeld der Technikgestaltung nicht allein Unternehmen und ihren Technikern überlassen.

Damit aber die Politik die eingangs gestellte Frage nach den Profiteuren der digitalen Revolution, mit „wir alle“ beantworten kann, müssen digitale Nutzerrechte allgemein und der Datenschutz im Besonderen höchsten Stellenwert in der österreichischen und europäischen Politik bekommen. Sie müssen quasi „Chefsache“ werden!

3. Versäumnisse im aktuellen Regierungsübereinkommen

Um diese Maxime zu erreichen, ist viel zu tun. Das Arbeitsprogramm der österreichischen Bundesregierung für die Jahre 2013 bis 2018 enthält bspw kein eigenes Kapitel zu den digitalen NutzerInnenrechten bzw zum Datenschutz. Entsprechend groß ist der Aufholbedarf bei der Politikgestaltung dieses Bereichs.

Im Kapitel „Demokratie“ findet sich immerhin der Aufruf „Datenschutz modernisieren“. Gemeint ist damit allerdings Folgendes: „Die Ressourcen der Datenschutzbehörden sollen zur Erfüllung der Kernaufgaben optimal eingesetzt werden können. Deshalb sollen aufwändige bürokratische Registrierungsverfahren, wie sie derzeit normiert sind, auf das notwendige Maß reduziert werden.“ Hilfsmittel, die den Marktüberblick und damit vorsorgliches behördliches Einschreiten erleichtern würden, werden mit anderen Worten reduziert. Die äußerst schmalen Ressourcen werden den förmlichen Entscheidungen über Einzelbeschwerden gewidmet. Darüber hinaus hat sich die Regierung - mit einer Ausnahme - auf kein weiteres Vorhaben in Bezug auf eine Reform des österreichischen Datenschutzes und die Verhandlungen zu einer EU-Datenschutz-Verordnung verständigt. Positiv ist, dass auf Drängen von Verbraucherschützern „Scoring“ (die automatisierte Bewertung der Verbraucherbonität) gesetzlich - „möglichst durch Anpassung des Datenschutzgesetzes“ - geregelt werden soll.

Ins Kapitel „Arbeitsrecht“ hat die Forderung nach einem Arbeitnehmerdatenschutzgesetz keinen Eingang gefunden. Unter der Überschrift „Infrastruktur“ wird immerhin dazu aufgerufen, „die digitale Zukunft aktiv zu gestalten“. Erfasst sind hier jedoch vorrangig der Ausbau der Breitbandnetze und die Schließung der „Digitalen Kluft“ (zwischen Stadt/Land und Jung/Alt). Unter „Kunst und Kultur“ findet Datenschutz einmal Erwähnung: bei der Reform des Urheberrechtes ist dieser zu berücksichtigen.

An einigen Stellen nimmt sich die Regierung relativ Unbestimmtes vor, bspw „für eine sichere Welt einzutreten“ sowie „Menschenrechte und Rechtsstaatlichkeit“ zu fördern. Sie möchte **„**diplomatische Initiativen zur weltweiten Stärkung des Grundrechts auf Datenschutz“ unterstützen. Angestrebt wird, den Schutz kritischer Infrastrukturen, die Sicherheit des „Cyber-Raums“ und der Menschen im „Cyber-Space“ zu erhöhen. Mit einer „Cyberinitiative“ soll „Cyberkriminalität“ bekämpft und Datensicherheit gewährleistet werden. Die Arbeiten zu den EU-Richtlinien für Cyber-Sicherheit und zum Datenschutz (für Polizei und Justiz) werden vorangetrieben. Tatbestände und Sanktionen im „Cyberstrafrecht“ werden evaluiert.

Das Übereinkommen enthält die Feststellung „Zusammenarbeit von Sicherheitsbehörden und –diensten ist im Interesse der Sicherheit notwendig, etwa für die Vermeidung und Bekämpfung von Extremismus und terroristischen Aktivitäten. Es gibt aber auch nachteilige (zB nachrichtendienstliche) Aktivitäten.“ Daraus formuliert die Regierung ihr Ziel eines „wirksamen Schutzes der Grund- und Freiheitsrechte der Menschen und der Integrität souveräner hoheitlicher Prozesse“. Das Amtsgeheimnis soll unter Berücksichtigung des Datenschutzes durch Open-Government-Regeln ersetzt werden. Schließlich wird noch ein Bekenntnis zum österreichischen Bankgeheimnis „im Sinne eines umfassenden Datenschutzes“ abgegeben.

Den Herausforderungen der digitalen Welt wurde nicht nur kein eigenes Kapitel gewidmet, auch die über das Übereinkommen verstreuten einschlägigen Projekte sind überschaubar: „Ausbau und Stärkung der e-Partizipation“ steht im Kapitel Jugend. Die Medienpolitik nimmt sich vor, „im Zuge des Wandels der Medienwelt ausgelöst durch die Digitalisierung“ unabhängige und vielfältige österreichische Medien zu sichern. Im Justizkapitel werden „moderne Regeln für eine moderne Gesellschaft“ und die Stärkung des Verbraucherrechts postuliert. Ob diese Gemeinplätze auch digitale Nutzerrechte umfassen sollen, liegt im Auge des Betrachters.

Insgesamt bleiben die Ziele weit hinter den Bedürfnissen und Erwartungen von ArbeitnehmerInnen, KonsumentInnen, InternetnutzerInnen und allgemein von BürgerInnen zurück. Die folgende Zusammenfassung offener Anliegen erhebt alles andere als den Anspruch der Vollständigkeit. Sie könnte selbstverständlich um unendlich viele weitere Aspekte ergänzt werden. Allein die Dynamik der Technologie- und Marktentwicklung zwingt natürlich geradezu zu laufenden Anpassungen.

4. Zentrale Bedürfnisse und Erwartungen in Kürze

Konkret erhoffen sich BürgerInnen, nicht zuletzt in ihrer Rolle als KonsumentInnen, ArbeitnehmerInnen, private wie berufliche NutzerInnen des Internets

- **Transparenz über alle Datenverarbeitungsvorgänge**, die derzeit abseits ihrer Wahrnehmung stattfinden. Mehr Transparenz braucht es aber auch in anderen Zusammenhängen: bspw in Bezug auf die Kriterien der Reihung von Suchmaschinenergebnissen, bei Bewertungsplattformen, bei denen unklar ist, ob Produktempfehlungen nicht manipuliert wurden oder Inhalten, die mangels Kennzeichnung redaktionellen Ursprungs sein können, aber genauso gut simple Werbung.

- **Rechtssicherheit in Bezug auf (un-)zulässige Datennutzungen.** Dazu gehören klar umrissene Zulässigkeitsgrenzen für die Datenverarbeitung und auch ausdrückliche Verarbeitungsverbote. Einzelfallsabwägungen bezüglich überwiegender Geheimhaltungs- oder Nutzungsinteressen an den jeweiligen Daten, die erst im Streitfall die Gerichte und Datenschutzbehörden vornehmen, sollten eher die Ausnahme sein.

- **eine starke Orientierung am Prinzip der Datensparsamkeit**. Nicht alle Datenverwertungen, die denkmöglich, bequem und zur Erreichung berechtigter Ziele auch nützlich sind, sind durch ein überwiegendes berechtigtes Interesse legitimiert. Die Einholung einer Zustimmung bei den Betroffenen verschafft einer Datennutzung auch nicht immer die nötige Legitimität. Denn typischerweise besteht ein erhebliches Kräfteungleichgewicht zwischen den Parteien. Von einer freiwilligen Zustimmung kann in diesem Fall nicht die Rede sein. Das Ziel, eine ausgewogene Balance zwischen Geheimhaltungs- und Nutzungsinteressen herzustellen, wird mit Zustimmungsklauseln oft nicht erreicht. Datensparsamkeit muss ein Maßstab sein, der in der Verwaltung und im Wirtschaftsleben ernsthafter angelegt wird, um die Frage nach der Zulässigkeit einer Datennutzung zu beantworten. Unter Umständen kollidierende Grundrechte, wie jene auf Achtung von Informations- und Eigentumsfreiheit, die auch die freie Entfaltung wirtschaftlicher Tätigkeiten umfasst, sind selbstverständlich zu beachten. Die nötige Rücksichtnahme auf andere Grundrechte ändert aber nichts daran, dass gerade der Datenschutz eine Stärkung benötigt, soll er nicht völlig ins Hintertreffen geraten.

- **Prävention vor Repression:** Vorbeugender Datenschutz durch behördliche Vorabkontrollen sollte deutlich ausgebaut werden. Eine spätere Feststellung von Datenschutzverstößen und Schäden bietet keinen gleichwertigen Ersatz für eine möglichst umfangreiche Verhinderung von Rechtsverletzungen. Dazu zählt auch der vorbeugende Missbrauchsschutz durch konkrete Datensicherheitspflichten. Bei dieser darf nicht gespart werden, auch wenn Datensicherheit im Einzelfall erhebliche Kosten verursacht.

- **Mehr Schutz gegenüber dominanten Internetkonzernen,** die in Drittstaaten, vor allem den USA, niedergelassen sind. Quasi-Monopole wie Google, Apple, Facebook uä. verfügen über eine fast unbeschränkte Marktmacht, weltweite Präsenz und Kundendaten in gigantischem Umfang. Die EU muss deshalb sicherstellen, dass diese „Over-the-Top-Player" auch datenschutzrechtlich mehr Verantwortung übernehmen. Im Wettbewerbsrecht hat die Europäische Kommission schon öfter bewiesen, dass es durchaus möglich ist, gegen große internationale Konzerne vorzugehen, wenn diese sich nicht an Regeln halten. Die Prozesse haben auch Beispielwirkung für andere Firmen. So wäre vielleicht eine einmalige Durchsetzung des Datenschutzrechts in diesem Bereich ausreichend, um alle Marktteilnehmer davon zu überzeugen, dass die Einhaltung der Datenschutzstandards in Europa nicht optional ist. Dazu ist auch eine starke Zusammenarbeit der nationalen Daten- und Konsumentenschutzorganisationen unter Einbeziehung der EU-Kommission nötig. Als Alternative zu „Gratis"-Diensten im Internet, die letztlich mit persönlichen Daten abgegolten werden, sind auch Bezahloptionen für Personen, die kein Profiling wollen, zu forcieren. Freilich erfordert dies engmaschige Kontrollen, damit das Vertrauen bezahlender Kunden in den Schutz ihrer Privatsphäre nicht missbraucht wird.

- **Spürbare Sanktionen bei systematischen Datenschutzverstößen.** Derzeit müssen Datenverwender weder mit einer (raschen) Aufdeckung illegaler Datennutzungen noch mit abschreckenden Strafen rechnen. Staatliche Kontrollen erfolgen bestenfalls punktuell. In der Regel wird erst aus Anlass massiver Beschwerden oder Medienberichte geprüft. Dann werden oft Verstöße bloß festgestellt. Die Verhängung von (nennenswerten) Strafen ist absolut rar. Aufsicht und Sanktionen müssen an Wirksamkeit drastisch zulegen. Andernfalls droht dem Datenschutz praktische Bedeutungslosigkeit.

- **Leichter Zugang zum Recht**. Jedermann muss sich bei vermuteten Verstößen an eine Datenschutzbehörde wenden können, die möglichst niedrigschwellig Rat erteilt und Rechtsschutz gewährt. Die derzeitige Zersplitterung der Zuständigkeiten zwischen der Datenschutzbehörde und den Zivilgerichten ist überholt. Für die Betroffenen stellt der Gang zu den Zivilgerichten ein kostenintensives Zugangshemmnis dar. Eine zeitgemäße Datenschutzbehörde muss demgegenüber einheitliche Anlaufstelle für Beschwerden über Verarbeitungen im öffentlichen und im privatwirtschaftlichen (unternehmerischen) Bereich sein.

- **Eine schlagkräftige Aufsichtsbehörde:** Ausstattung und technisches Knowhow der Datenschutzbehörde muss mit den hohen Anforderungen an ein solches Kontrollorgan Schritt halten können. Angesichts millionenfacher Datenverarbeitungen braucht die Behörde Unterstützung, um einen Marktüberblick zu haben. Dazu zählen ein effizient geführtes Datenverarbeitungsregister und Datenschutzbeauftragte in möglichst allen österreichischen Betrieben. Die gegenwärtige Praxis: viele Verantwortliche kommen ihren Registermeldepflichten nicht nach. Die verpflichtende Einrichtung betrieblicher Datenschutzbeauftragter scheitert am Widerstand der Wirtschaftsseite. Die Publizität von heiklen Datenverarbeitungen und ein dichtes Netz an betrieblichen Datenschutzbeauftragten ist freilich Voraussetzung für eine erfolgreiche Kontrolltätigkeit.

- **Staatliche Souveränität statt Spielball von Geheimdiensten**: Die drängendsten Fragen über die Arbeitsmethoden von Geheimdiensten und des genauen Umfangs von geheimdienstlichen Datenschutzverstößen in Telekommunikationsnetzen sind rasch zu klären. Die parlamentarische Kontrolle von Geheimdiensten ist zu reformieren.

- **Mehr Schutz vor Internetkriminalität,** zB durch ressortübergreifende Schwerpunktaktionen, Schwerpunktstaatsanwaltschaften für den Cybercrime-Bereich und finanzielle Förderungen für die Aufklärungsarbeit, die bspw die „Watchlist Internetbetrug“ leistet.

- **Faire Nutzerrechte in Bezug auf urheberrechtlich geschützte digitale Güter,** etwa durch Absicherung konkret durchsetzbarer freier Werknutzungsrechte wie digitale Privatkopien, einen tatsächlich freien Binnenmarkt und spezifische Gewährleistungsregeln für digitale Güter, Schutz vor einer „Abmahnindustrie“, die private Internetnutzer wegen tatsächlicher oder vermeintlicher Rechtsverletzungen mit überhöhten Forderungen verfolgt, und im Zuge der Rechtsverfolgung geistigen Eigentums einen Richtervorbehalt für alle Grundrechtseingriffe gegenüber InternetnutzerInnen.

- **Ein Zentrum für netzpolitische Studien.** Regierung, Parlament, aber auch Interessenvertretungen von Verbrauchern und ArbeitnehmerInnen benötigen ein Kompetenzzentrum, das dabei unterstützt, alle digitalen Entwicklungen im Detail zu erfassen und zu bewerten. Technische Studien, Marktüberblicken, nutzerInnenbezogene Praxistests und Handlungskonzepte schaffen die Grundlagen für die rechtspolitische Arbeit.

5. Die österreichische Regierung muss sich für eine EU-Datenschutz-Verordnung auf hohem Niveau einsetzen

Bewährte allgemeine Regeln beibehalten, digitale Spezialthemen regeln

Die geltende Datenschutz-Richtlinie stammt aus dem Jahr 1995. Sie baut auf sehr allgemeinen Datenschutzprinzipien auf. Diese sind „zeitlos" anwendbar. Sie können als genereller Rahmen weitgehend unverändert beibehalten werden. Die größte Schwachstelle des bisherigen Regimes ist allerdings seit Jahren der mangelhafte Vollzug der Datenschutzregeln. Damit Datenschutz an praktischem Gewicht gewinnt, muss die Rechtsdurchsetzung massiv verbessert werden. Das Datenschutzrecht wird den digitalen Herausforderungen nur gewachsen sein, wenn es auch auf die fortschreitende Digitaltechnik und ihrem Gefährdungspotential für die Privatsphäre möglichst konkret eingeht.

1995, im Entstehungsjahr der Richtlinie, gab es weder die Begriffe noch einen Regulierungsbedarf für damals unbekannte oder nicht weitentwickelte Phänomene wie

- **„Always on" über Smartphones und Breitbandinternet,**
- **Big Data Analysen, Datamining, Scoring und Profiling,**
- **Digitale Marktforschung durch individuelles Tracking, verhaltensbasierte Onlinewerbung**
- **Speichern in der Cloud**
- **Cyber-Sicherheit**
- **das „Mitmach"-Web 2.0**
- **Netzkonflikte zwischen Informationsfreiheit und dem Datenschutz**
- **Online-Überwachungsexzesse durch Geheimdienste uvm**

Themenspezifische Datenschutzregeln müssen daher die allgemeinen Grundsätze ergänzen. Damit werden die allgemeinen Vorgaben für das jeweilige Anwendungsfeld präzisiert. Wann liegt etwa im jeweiligen Zusammenhang ein „überwiegendes berechtigtes Interesse" an einer Datennutzung vor? Welcher Eingriff in Geheimhaltungsinteressen ist unter welchen Umständen „verhältnismäßig"? Was ist bei Wahl der Mittel der „schonendste" Eingriff? Was ist die für den jeweiligen Speicherzweck maximale Speicherdauer uvm?

Ziel ist, dass InternetnutzerInnen und andere Betroffene eine klare Vorstellung von ihren Rechten und Pflichten bekommen. Angesichts des extremen Kräfteungleichgewichts gegenüber Online-Datensammlern und den vielen rechtlichen Grauzonen im Internet sind klarere Ge- und Verbote nötig. So fehlen bspw Detailregeln für soziale Netzwerke, App-Plattformen und –Entwickler, Suchmaschinen, geobasierte Dienste, Verhaltensprofile im Web, Scoring und Direktmarketing. Aber auch die Bereiche des Arbeitnehmerdatenschutzes oder der Umgang mit Daten in verschiedenen öffentlichen Sektoren verdienen viel mehr Aufmerksamkeit.

Der Kommissionsentwurf zur Datenschutz-Grundverordnung

Der von der EU-Kommission vorgelegte Entwurf für eine zeitgemäße Datenschutzverordnung enthält fortschrittliche Ideen. Er gibt aber auch Anlass zur Kritik. Während das EU-Parlament sich einigermaßen verdienstvoll um Verbesserungen bemüht, setzen die Änderungsvorschläge im Rat das geltende Datenschutzniveau sogar herab. Vor diesem Hintergrund ist eine kritische Haltung Österreichs erforderlich. Denn es besteht die Gefahr, dass das Vorhaben eines fortschrittlichen, strengen Datenschutzes vor allem an der Haltung des Rats scheitert.

Was jedenfalls zu regeln ist…

Anonymisierungsgebot: Ist die Notwendigkeit eines Personenbezugs nicht eindeutig nachgewiesen, sind Daten vor ihrer Nutzung restlos zu anonymisieren. Das Prinzip der Datensparsamkeit gebietet diese Vorgangsweise. Dies muss in der Verordnung auch klar zum Ausdruck kommen. Vorgaben wie „soweit die Verarbeitungszwecke die Identifizierung des Betroffenen nicht erfordern, soll der Auftraggeber nicht verpflichtet sein, zusätzliche Daten zur Identifizierung zu speichern“ greifen zu kurz. Benötigt wird ein Verbot, dass „wenn der Zweck der Verarbeitung es nicht erfordert, der Auftraggeber keine Identifizierung vornehmen darf.“

Pseudonymisierung als Ausnahmefall: Als „pseudonymisierte Daten“ gelten personenbezogene Daten, die einer Person ohne zusätzliche Informationen nicht eindeutig zugeordnet werden können. Derartige Zusatzinformationen sind getrennt aufzubewahren. Ihre Zuordnung zu einer konkreten Person muss durch technische bzw organisatorische Maßnahmen unterbunden werden. Oft werden anonymisierte und pseudonymisierte Daten in einem Atemzug genannt. Erstere weisen aber keinerlei Personenbezug auf. Ein solcher ist für den Datennutzer auch nicht mehr herstellbar. Auf die letztere Datenkategorie trifft das nicht zu: der Datennutzer kann den Personenbezug - unter Abgehen von der allenfalls getroffenen Übereinkunft, keine Identifizierung vorzunehmen – wieder herstellen. Für die Pseudonymisierung gibt es zweckmäßige Anwendungsgebiete (zB bei der Anmeldung von Internetforen-NutzerInnen, damit in speziell geregelten Fällen – wie etwa strafrechtlichen Verstößen von DienstenutzerInnen – die Pseudonymisierung vom Diensteanbieter aufgehoben und der Klarname an die zuständigen Behörden weitergegeben werden kann). Auch bei Zeitverlaufs-Studien wird darauf zurückgegriffen, um neue Sachverhalte einer individuellen Person im Zeitverlauf zuordnen zu können.

Rechtliche Erleichterungen für die Verwender pseudonymisierter Daten, wie vom Rat gewünscht, sind unangebracht. Pseudonymisierung erweckt oft den Eindruck einer Pseudosicherheit. In der Praxis ist eine vollständige Anonymisierung häufig möglich und rechtlich geboten. Im Wege einer Pseudonymisierung hält sich der Datennutzer hingegen die Tür zu einer personenbezogenen Nutzung (etwa durch Änderung seiner Geschäftsklauseln) offen. Pseudonymisierungszusagen eröffnen damit schwer kontrollierbare Missbrauchspotentiale.

Gesamtverantwortung des Auftraggebers einer Datenverarbeitung: Die EU-Kommission schlug vor, dass personenbezogene Daten „unter der Gesamtverantwortung des für die Verarbeitung Verantwortlichen“ verarbeitet werden, der dafür haftet, „dass bei jedem Verarbeitungsvorgang die Vorschriften dieser Verordnung eingehalten werden, und der den Nachweis hierfür erbringen muss.“ Ein expliziter Hinweis auf die Gesamtverantwortung und Beweispflichten ist hilfreich. Datennutzer sollen ihre Verantwortung im Konfliktfall nicht auf untergeordnete Datenverantwortliche und Dienstleister abzuwälzen versuchen.

Höhere Anforderungen an die Zustimmung zur Datennutzung: Für Verbraucher ist wichtig, dass die Zustimmung zur Nutzung ihrer personenbezogenen Daten künftig ausdrücklich erfolgen muss. Diese Änderung bedeutet eine deutliche Anhebung des bisherigen Datenschutzniveaus. Zustimmungen durch stillschweigende Akzeptanz von (nicht gelesenen) Geschäftsbedingungen würden der Vergangenheit angehören. Der Datennutzer muss sich jedenfalls um ein aktives Zeichen der KonsumentInnen bemühen, also das Setzen eines Hakens beim Anklicken eines Kästchens im Internet oder Einholen der Unterschrift. Die Einwilligung muss erkennbar und von anderen Texten getrennt sein. Voreingestellte Haken, die der Nutzer entfernen muss, sollten unzulässig sein.

Versuchen, diese Anforderungen wieder aufzuweichen, ist eine Absage zu erteilen. So ist eine „unzweifelhafte“ zB nicht einer „ausdrücklichen“ Zustimmung gleich zu halten.

Mehr Schutz vor Direktmarketing: KonsumentInnen fühlen sich durch Direktwerbung oft belästigt. Viele der im Internet eingesetzten Tracking-Methoden sind intransparent und rechtswidrig. Die Anforderungen an Verhaltensprofile von InternetnutzerInnen und das Direktmarketing sollten unbedingt verschärft werden. Eine ausdrückliche Zustimmungspflicht zur Datennutzung muss gerade auch für diesen intransparenten Bereich gelten. Eine Privilegierung des Direktmarketings durch eine bloße Opt-Out-Regel darf es nicht geben. Dabei stünde dem Verbraucher gegen die Verwendung seiner Daten zu Werbezwecken nur ein Widerrufsrecht zu. Sämtliche Lippenbekenntnisse, Datenschutz im Internet verbessern zu wollen, verlieren an Glaubwürdigkeit, könnten Direktwerbeunternehmen, also etwa Google, sich über die Souveränität der Internetnutzer in Bezug auf ihre Daten hinwegsetzen und Daten ohne explizite Zustimmung für Werbezwecke nutzen. Dazu kommt, dass nicht einmal die Datenarten geregelt sind, die von diesem Nutzungsprivileg erfasst wären. Eine Opt-Out Regelung für Direktwerbung ist unakzeptabel. Das Versprechen nach einem zeitgemäßen Datenschutz im Internet würde so nicht ansatzweise eingelöst werden.

Keine „unfreiwilligen“ Zustimmungen: Einwilligungen dürfen nicht wirksam sein, wenn zwischen den Positionen des Betroffenen und des Datenverarbeiters ein besonderes Kräfteungleichgewicht besteht. Dies muss für Arbeitnehmerverhältnisse gelten. Ungleiche Machtverhältnisse bestehen aber auch bei Verbrauchergeschäften. Unternehmen verweigern häufig Vertragsabschlüsse, wenn KonsumentInnen einer Datennutzung für Marketingzwecken nicht zustimmen. Die Freiwilligkeit einer Zustimmung ist daher auch hier anzuzweifeln. Mit einem Koppelungsverbot dürften Konsumenten vom Bezug der Ware oder Dienstleistung nicht mehr ausgeschlossen werden, wenn sie einer für die Vertragserfüllung unnötigen Datennutzung nicht zustimmen. Wichtig ist das vor allem dann, wenn es keine Alternativangebote am Markt gibt.

Klare Ge- und Verbote statt unbestimmter Erlaubnistatbestände: Die Datennutzung soll nach dem Wunsch von Kommission, Parlament und Rat auch „im überwiegenden berechtigten Interesse“ des Auftraggebers (oder Empfängers) erfolgen können. Dieser Regelungsansatz ist unbestimmt, bietet wenig Rechtssicherheit und kann auch unvertretbar weit ausgelegt werden. Deshalb sind die Datennutzungen anzuführen, bei denen typischerweise von einem solchen überwiegenden Interesse auszugehen ist. Daneben sind Fälle aufzulisten, wo dies ausgeschlossen wird.

Datennutzung nur im Rahmen des Ursprungszweckes: Es muss klar sein, dass Daten nicht für Zwecke genutzt werden dürfen, die mit dem originären Speicherzweck nicht in Einklang stehen. Ausnahmen von diesem Verbot (wie die Verarbeitung für statistische oder historische Zwecke) sind restriktiv zu handhaben und abschließend anzuführen. Möchte jemand Daten über den ursprünglichen Zweck hinaus für andere Zwecke weiternutzen, benötigt er dafür eine eigene Rechtsgrundlage (zB die Zustimmung der Betroffenen). Benötigt wird daher ein Weiterverarbeitungsverbot für andere Zwecke plus weniger begründeter Ausnahmen. Vage Kriterien, die bei der Abwägung unterstützen sollen, werden abgelehnt.

Ausdehnung des EU-Datenschutzes auf Drittländer: Die Anwendbarkeit der künftigen Datenschutz-Verordnung soll auf Anbieter aus Drittländern, zB US-Internetdienste, ausgedehnt werden. Wenn US-Anbieter europäische NutzerInnen haben oder Kundenprofile anlegen wollen, ist das wichtig.

Die Einbeziehung ist bedeutsam, da vielen Internetangeboten von großer Reichweite und datenschutzrechtlicher Brisanz oft keine europäische Niederlassung zurechenbar ist. Gleichzeitig müssen aber auch Vollstreckungsübereinkommen mit den USA vorangetrieben werden, andernfalls werden vorhandene Rechtsansprüche europäischer BürgerInnen weiterhin schwer durchsetzbar sein.

Kinder- und Jugendschutz: Die Verarbeitung von Daten über Kinder knüpft die EU-Kommission an die Bedingung, dass bis zum 13. Lebensjahr die Eltern der Datenverarbeitung bei Internetdiensten zustimmen müssen. Der Dienstanbieter muss auch Anstrengungen unternehmen, dass das Vorliegen der elterlichen Einwilligung nachprüfbar ist. Mit Blick darauf, dass die Geschäftsfähigkeit in Österreich - abgestuft für die Altersgruppen bis 14 und 18 Jahre - beschränkt ist, sollte die Voraussetzung einer elterlichen Genehmigung auf ein höheres Alter ausgedehnt werden.

Automatische Verbraucherinformation: Von Verarbeitungen Betroffene müssen vor der Datenermittlung mehr Informationen vom Datennutzer erhalten. KonsumentInnen muss bei der Datenerhebung bzw innerhalb einer angemessenen Frist u.a. mitgeteilt werden: neben dem Namen und den Kontaktdaten des Datenverantwortlichen, die Nutzungszwecke, auch die konkrete Speicherdauer, die Herkunft der Daten, ob die Bereitstellung der Daten verpflichtend oder freiwillig ist uä. Diese Maßnahme dient der Transparenz und ist die unbedingte Voraussetzung dafür, dass KonsumentInnen ihre Rechte in der Praxis wahrnehmen können. Ohne Kenntnisse, wer welche Daten wozu verarbeitet, können Betroffene auch von ihren Auskunfts-, Widerrufs-, Löschungs- und Berichtigungsrechten nicht Gebrauch machen. Diese Informationen dürfen nur entfallen, wenn die Realisierung unmöglich ist - nicht aber auch, soweit sie bloß mit einem „unverhältnismäßig hohen Aufwand“ verbunden ist. Diese Einschränkung höhlt den Schutz aus. Es führt zu Rechtsunsicherheit, weil die Frage nach der Zumutbarkeit eines Aufwands – ohne unternehmensinterne Kenntnisse - weder vom Betroffenen noch von den Datenschutzbehörden verlässlich beurteilt werden kann.

Dem Vorhaben des Rates, die Speicherdauer aus dem Katalog der Informationspflichten zu streichen, ist eine klare Absage zu erteilen. Die Information darf auch nicht entfallen, wenn nach dem Ansinnen des Rates „dadurch das Erreichen der Speicherabsichten beeinträchtigt würde“. Im Anwendungsbereich der Verordnung sollte absolute Transparenz herrschen. Anliegen der öffentlichen Sicherheit fallen nicht unter die Verordnung und entfallen deshalb als Begründung.

Lückenloses Auskunftsrecht: Das Recht auf Auskunft muss jederzeit - zumindest einmal jährlich – und in jeder Hinsicht kostenlos ausgeübt werden können. Zeitliche Einschränkungen (wie etwa innerhalb „vernünftiger, angemessener Intervalle“) sind abzulehnen. Selbstverständlich müssen im Rahmen der Auskunft auch die einzelnen Datenarten angeführt werden. Alles andere würde einen massiven Rückschritt zur geltenden Rechtslage bedeuten. Die Möglichkeit des Auskunftssuchenden, eine „Kopie“ der Daten anzufordern, ist kein gleichwertiger Ersatz. Sie ist mit einer Kostenpflicht verbunden und kann verweigert werden, wenn in Textteilen Daten Dritter enthalten sind. Die Ausübung des Auskunftsrechts darf nicht daran scheitern, dass nur eine „Kopie“ der Datenanwendung herauszugeben ist und die Herausgabe verweigert werden kann, wenn dritte Personen aufscheinen. Dann muss der Auftraggeber den Dateninhalt, soweit es den Auskunftswerber betrifft, zusammengefasst wiedergeben. Ein Rückschritt gegenüber dem Status Quo ist undenkbar.

Strikte Auskunftspflicht über die Datenherkunft und Empfänger: Die Auskunftspflicht bezüglich der Herkunft von Daten bezieht sich nur auf „verfügbare“ Daten. Das hat zur Folge, dass - ohne lückenlose Dokumentationspflicht - es in der Hand der Datenverantwortlichen liegt, ob sie Auskünfte zur Datenquelle (vollständig) erteilen oder nicht. Datennutzer haben derzeit auch bloß über „Empfänger oder Empfängerkreise“ zu informieren. Die Aussagekraft zwischen diesen beiden Kategorien kann unterschiedlicher nicht sein. Der Verpflichtung wird schon entsprochen, wenn die Branche (zB „Finanzdienstleister“) offengelegt wird. Der Betroffene kann seine Rechte nur ausüben, wenn das jeweilige einzelne Unternehmen benannt wird. Daher sind grundsätzlich die Empfänger namhaft zu machen. Die Angabe bloßer Empfängerkreise reicht nur in Verbindung mit einer schlüssigen Begründung, weshalb die konkreten Empfänger ausnahmsweise nicht bekannt sind.

Spezielle Löschungsrechte im Internet: FacebooknutzerInnen veröffentlichen massenhaft Personendaten über sich und Dritte. Es bedarf daher eines Rechtsanspruchs auf vollständige Datenlöschung im Internet, also auf Wunsch wieder „vergessen zu werden“. Ein Fortschritt wäre auch die Verpflichtung desjenigen, der personenbezogene Daten im Internet veröffentlicht hat, „alle vertretbaren Schritte“ zu setzen, Dritte, die diese Daten weiterverarbeiten, darüber zu informieren, dass der Internetnutzer die Löschung aller Querverweise und Kopien verlangt hat. Der Entwurf regt auch zu datenschutzfreundlichen Voreinstellungen bei Internetdiensten an. Das ist zahnlos. Betreiber müssen ihre Privatsphäre-Werkzeuge streng voreinstellen, also so, dass etwa in Sozialen Netzwerken Daten nur den „FreundInnen“ nicht aber der Öffentlichkeit zugänglich sind.

Der Kommissionsentwurf enthält als eine der zentralen Verbesserungen zum Status Quo auch „Rechte gegenüber Empfängern“. Es ist zeitgemäß und wichtig, Betroffene von der Last zu befreien, eine Löschung auf allen Ebenen einer Übermittlungskette allein durchsetzen zu müssen. Von folgender Verpflichtung darf deshalb nicht abgesehen werden: „Der für die Verarbeitung Verantwortliche muss allen Empfängern, an die Daten weitergegeben wurden, jede Berichtigung oder Löschung ….mitteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.“

Strikte Löschroutinen: Dem Kommissionsvorschlag zufolge „hat der für die Verarbeitung Verantwortliche Vorkehrungen zu treffen, um sicherzustellen, dass die Fristen für die Löschung personenbezogener Daten und/oder die regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung eingehalten werden.“ Damit sind elementare Sorgfaltspflichten zwar nicht präzise geregelt, aber zumindest angesprochen. Eine Eliminierung - wie vom Rat vorgeschlagen - kommt nicht in Frage.

Umfangreiches Widerspruchsrecht: Für die erfolgreiche Ausübung des Widerspruchsrechts gegen eine Datenverarbeitung sind der Bestimmung zufolge „Gründe, die sich aus einer besonderen Situation ergeben“ anzuführen. Ein begründungsloses Widerspruchsrecht gibt es offenbar nur für den Fall der Direktwerbung. Unbedingt hinzuzufügen ist, dass einmal erteilte Zustimmungen vom Betroffenen jederzeit widerrufen werden können. Auf dieses Widerrufsrecht hat der Auftraggeber den Betroffenen auch hinzuweisen. Außerdem muss Betroffenen ein begründungsloses Widerspruchsrecht zustehen, wenn - wie nach geltender Rechtslage - die Daten in eine gesetzlich nicht angeordnete, aber öffentlich zugängliche Datenanwendung aufgenommen worden sind.

Klare Grenzen für Profilbildung und Personenbewertung: Die Vorschläge von Kommission, Parlament und Rat schaffen einen breiten Erlaubnistatbestand für die an Scoring und Profiling interessierte Wirtschaft. Datenschutz und Rechtsschutzanliegen der Verbraucher kommen dabei zu kurz. Unter dem Titel „Profiling" werden nicht alle heiklen Datennutzungen erfasst, bei denen automatisierte Einzelentscheidungen getroffen werden. Es ist daher wichtig, dass nicht nur für die Bildung von gesamten Personenprofilen, sondern auch für die Bewertung von bestimmten Einzelmerkmalen von Personen (zB Finanzkraft, Vorlieben, Gesundheit usw.) und Verhaltensprognosen (wie zB erwartetes Zahlungsverhalten, Kaufhäufigkeit) durch Datenanalyse- und Prognoseinstrumente Regelungen getroffen werden.

Die bisher am Tisch liegenden Vorschläge erfassen die gegenwärtigen (und umso mehr noch die künftigen) Probleme mit dem unverhältnismäßigen Einsatz von Datamining – und Scoring-Methoden nicht ansatzweise. Entscheidende Fragen werden ausgeklammert: unter welchen Voraussetzungen dürfen Personenprofile und Scores überhaupt gebildet werden? Welche Datenarten dürfen maximal verarbeitet werden? Welche Anforderungen stellt man an die wissenschaftliche Aussagekraft und Haltbarkeit von Prognosewerkzeugen, damit Betroffene nicht willkürlichen und diskriminierenden Verhaltenszuschreibungen ausgesetzt sind?

Angesprochen werden immerhin die Informations- und Auskunftsrechte der Betroffenen. Mit keinem Wort erwähnt werden aber die Besonderheiten, die bei der Ausübung des Auskunftsrechtes zur berücksichtigen sind (etwa in Bezug auf die in die Gesamtbewertung der Person einfließenden Kriterien und Gewichtungen). Keinesfalls zuzustimmen ist der Einschränkung, dass Auskunft über die Logik und die Folgen des Einsatzes einer Scoringsoftware Betroffenen nur zu erteilen ist, wenn Geschäfts- und Betriebsgeheimnisse der Auskunftserteilung nicht entgegenstehen. Das widerspricht dem Bedürfnis der Verbraucher nach einer vollständigen, transparenten Auskunft. Die Vorschläge lassen offen, wann eine automatisierte Entscheidungsfindung überhaupt „notwendig" ist (es fehlen etwa Bagatellgrenzen, eine Beschreibung der Vertragstypen, Branchen etc). Die Zulässigkeit einer Profilbildung und einer Personenbewertung darf keinesfalls nur auf der Zustimmung des Betroffenen aufbauen. Es darf nicht ernsthaft angenommen werden, dass in diesem Kontext die Zustimmung des Verbrauchers jemals freiwillig erfolgt.

Kurz, es fehlt an vielem, etwa: der Beschränkung des zulässigen Datenumfangs auf harte Negativdaten, wie Zahlungsanstände, dem Verwendungsverbot von Daten von Direktwerbeunternehmen und Medieninfos über Privatpersonen, Bagatellgrenzen, Regeln für automatisierte Bewertungen (Diskriminierungsverbot, Transparenzgebot, unabhängige Zertifizierung uvm), Informationspflichten vor der Datenermittlung gegenüber den Betroffenen, der Protokollierung der Datenherkunft und der Empfänger, dichten Aktualisierungen des Datenbestandes, präzisen Löschfristen und einer branchenfinanzierten Schlichtungsstelle.

Datenverarbeiter sollen mehr Eigenverantwortung übernehmen: Die EU-Kommission möchte Datennutzer stärker in die Verantwortung nehmen – durch verpflichtende Dokumentationen, Sicherheitsmaßnahmen, Datenschutzbeauftragte und eine Risikoabschätzung bei heiklen Datenanwendungen etwa bei Personenprofilen und der Nutzung von Gesundheitsdaten. Behördenaufgaben werden damit zwar „privatisiert". Klar ist aber auch: Datenschutzbehörden können nicht Millionen Datenanwendungen gleichzeitig im Auge behalten und sind derzeit auf Beschwerden angewiesen. Viele Verarbeitungen finden ohne Wissen der KonsumentInnen „hinter den Kulissen" statt, weshalb nicht allein auf das Einlangen von Anzeigen gesetzt werden kann. Der EU-Kommissionsentwurf enthält gute Ansätze. Die Ausgestaltung der Vorschriften ist jedoch so mangelhaft, dass sie kaum Nutzen stiften.

Unausgereifte Regeln über Dokumentationspflichten und Risikoanalysen sowie verpflichtende Datenschutzbeauftragte ausschließlich in Betrieben mit extrem hoher Beschäftigtenzahl schaffen keinen Ausgleich für einen Wegfall der Transparenz- und Kontrollbestimmungen (Meldeverfahren und Vorabkontrolle) nach der gegenwärtigen Rechtslage. Deshalb braucht es mehr: Datenverarbeiter sollen sensible Vorhaben auf eigene Kosten durch unabhängige Begutachtungsstellen prüfen lassen, damit Datenschutzkonformität im Großen und Ganzen gewährleistet ist (ob ein Vorhaben als datenschutzrechtlich „heikel“ einzustufen ist, sollten die Datenschutzbehörden entscheiden).

Melderegister beibehalten: Auf die Eigenverantwortung des Datennutzers zu setzen, darf nicht dazu führen, dass bisherige Kontrollvorschriften wie das Meldeverfahren und die behördliche Vorabkontrolle komplett aufgegeben werden. Das Melderegister erfüllt einen wichtigen Publizitätszweck (Verbraucher können Einsicht nehmen) und gewährt der Datenschutzbehörde einen Einblick in die Verarbeitungspraxis. Angesichts der Masse an Meldungen (und leider auch rechtswidrig unterlassenen Registrierungen) kann die Datenschutzbehörde die gemeldeten Datennutzungen zwar nicht generell auf ihre Rechtskonformität überprüfen. Im Beschwerdefall bzw im Rahmen von Stichproben sollen Meldungen ans Datenverarbeitungsregister aber geprüft werden.

Risikoabschätzungen nicht allein dem Datennutzer überlassen: Risikoabschätzungen sollten der Ursprungsabsicht der EU-Kommission zufolge vor dem Beginn der Datenverarbeitung erfolgen und der Öffentlichkeit leicht zugänglich gemacht werden. Davon ist schon nicht mehr die Rede. Außerdem sind die Regeln zu unausgereift, um Rechtssicherheit zu bieten, wann, in welchem Umfang und was zu prüfen ist. Im ungünstigsten Fall prüft sich der Geprüfte (ohne Einbindung der Datenschutzbehörde und Konsequenzen) selbst. Die Rolle der Datenschutzbehörde ist unklar. Auch bei einer betriebsinternen Folgenabschätzung ist die Datenschutzbehörde formell einzubinden und mit Kontroll- und Gestaltungsrechten auszustatten. Verarbeitungen sind ihr weiterhin anzuzeigen. Nur so kann die Behörde Datennutzer zur Folgenabschätzung auch anhalten. Die Ergebnisse müssen ihr verpflichtend vorgelegt werden, damit die Behörde bei Bedarf Konsequenzen ziehen kann.

Privacy by Design: Datenschutz ist bei der Entwicklung neuer Technologien frühestmöglich miteinzuplanen. Neue Systeme bergen oft Datenschutzrisiken, die sich nur mehr schwer beseitigen lassen, wenn das Grundkonzept erst einmal feststeht. Der Ansatz, Datenschutz ins Gesamtdesign miteinzubeziehen (anstatt Datenschutzprobleme erst später zu beheben) ist wichtig. Der Kommissionsvorschlag bleibt aber zu unverbindlich, um in der Praxis Nutzen zu stiften. Es fehlen Vorgaben, wie bspw:

- **Datenvermeidung:** Datenverarbeitung ist so zu dimensionieren, dass keine bzw nur für den beabsichtigten Zweck unbedingt nötige personenbezogenen Daten verwendet werden.
- **Kontrolle:** IT-Systeme sollten den Betroffenen ermöglichen, ihre Daten zu kontrollieren. Die Abgabe von Zustimmungen bzw Widersprüchen zur Datennutzung sollten technisch vereinfacht werden.
- **Transparenz**: Entwickler und Betreiber müssen die Betroffenen detailliert über die Funktionsweise der Systeme informieren.
- **Vertraulichkeit:** nur autorisierte Personen dürfen Datenzugriff erhalten.
- **Datenqualität:** Prüfung zulässiger Datenquellen und Datenempfänger, Aktualisierungen, Löschroutinen
- **Trennung:** werden Data Warehouses oder Clouds benutzt müssen Daten sicher getrennt aufbewahrt werden.

Privacy by Default: Möglichst strenge Privatsphäre-Einstellungen bei Onlinediensten sind konkret und verbindlich vorzuschreiben, um wirklich dem Schutz von Internetnutzern zu dienen. Plattformbetreiber müssen zB die Standardeinstellung eines Profils in sozialen Netzwerken so wählen, dass nur der FreundInnenkreis Zugang hat. Dienstnutzer setzen sich nicht eingehend mit komplizierten Privatsphäre-Konzepten, die sie selbst (de-) aktivieren müssen, auseinander. Die Dienstanbieter profitieren von Voreinstellungen, mit denen sie die größtmögliche Veröffentlichung bzw Weitergabe von Daten verwirklichen. Die Grundeinstellungen für die Privatsphäre eines Dienstes müssen also standardmäßig so restriktiv sein, dass Datenzugriffe minimiert werden.

Pflicht zur Meldung schwerwiegender Datenpannen: Diese Meldepflicht sollte selbstverständlich sein, um der Datenschutzbehörde die rasche Einleitung eines amtswegigen Prüfverfahrens zu ermöglichen und Betroffene solcherart (aber auch durch eine individuelle Verständigung) vor weitergehenden Schäden zu bewahren. Für die vom Rat geforderten Ausnahmen von der Pflicht zur Meldung schwerwiegender Datenpannen gibt es keine sachliche Rechtfertigung. Ausnahmen wie „der Auftraggeber hat ohnedies technische Schutzmaßnahmen ergriffen“ sind entgegenzuhalten, dass sie sich offenbar als wirkungslos erwiesen haben. Auch wenn der Auftraggeber Maßnahmen ergriffen hat, die sicherstellen, dass „die Betroffenen nicht länger ernsthaft durch die Datenschutzverletzung berührt sind“, wollen die Betroffenen auch über eine zurückliegende Geheimhaltungsverletzung informiert sein. Und selbst wenn die Meldung „wichtigen öffentlichen Interessen widerspricht“, sollte Transparenz gegenüber den Geschädigten vorgehen.

Wirksame Rechtsdurchsetzung: Nötig ist Transparenz durch ein Datenverarbeitungsregister, eine Risikominimierung heikler Datennutzungen durch behördliche Vorabkontrolle und parallel dazu eine stärkere Verlagerung des Aufwands auf die Datenverarbeiter selbst (die Datenschutzbehörden sollen die Vorlage von Zertifizierungen, Risikoanalysen uä verlangen können). Neben dem Vertretungsrecht in datenschutzrechtlichen Verfahren sollte Einrichtungen, die die Interessen von ArbeitnehmerInnen und VerbraucherInnen wahrnehmen, eine Verbandsklagsbefugnis zukommen.

Behördenzuständigkeit ohne One-Stop-Shop: Das Konzept der ausschließlichen Zuständigkeit der Datenschutzbehörde am Ort der Hauptniederlassung würde den Betroffenen den Zugang zum Recht massiv erschweren. Mit der freien Wahl der Hauptniederlassung bleiben Datenschutzbehörden weiterhin Spielball von Konzernen. Nicht nur die zentrale Verwaltung innerhalb der EU, sondern auch der Ort, an dem Entscheidungen über „die Zwecke und Maßnahmen der Datenspeicherung“ getroffen werden, wäre für die örtliche Zuständigkeit maßgeblich. Das Vorhaben hätte zur Folge, dass die zuständige Behörde für ein beispielsweise in Österreich angesiedeltes Tochterunternehmen eines europaweit agierenden Konzerns nicht mehr die österreichische Datenschutzbehörde wäre, sondern die Datenschutzbehörde am Ort der ausländischen Hauptniederlassung des Konzerns. Damit kann ein in mehreren Mitgliedstaaten niedergelassenes Unternehmen leicht „Forumshopping“ zugunsten des Landes mit dem schwächsten Vollzug betreiben. Zwar können sich Betroffene weiterhin an ihre nationale Datenschutzbehörde als Anlaufstelle wenden, dieser käme aber keine Entscheidungsbefugnis im Falle von konzernweiten Datenverwendungen zu. An die Entscheidung der „leading“- Datenschutzbehörde wäre auch das nationale Gericht gebunden. Das Modell ist allgemein, vor allem aber im Zusammenhang mit dem Beschäftigtendatenschutz abzulehnen.

Behördliche Vorabgenehmigungen: BürgerInnen wünschen sich mehr Vorsorge. Die nachträgliche Feststellung von Verstößen und allfällige Ersatzleistungen können Präventivmaßnahmen nicht ersetzen. Dem Kommissionsentwurf zufolge hat der „Verantwortliche vor der Verarbeitung…eine Genehmigung der Aufsichtsbehörde einzuholen, um sicherzustellen, dass die geplante Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt, und insbesondere die Risiken (bei Drittlandsübermittlungen) zu mindern….". Geplanten Streichungen ist eine Absage zu erteilen. Eine Vorabgenehmigung bei besonders sensiblen Datenanwendungen ist dringend notwendig, da eine bloße ex-post Aufsicht das bisherige Datenschutzniveau noch weiter senken würde.

Datenschutzbehörde als „Consultant": Absolut zu unterstützen ist der Ansatz, dass ratsuchende Datenverarbeiter die Datenschutzbehörde auch (gegen Kostenersatz) konsultieren können. Abseits förmlicher Behördenentscheidungen muss die Möglichkeit eines institutionalisierten Dialogs zwischen Datenverarbeitern und ihrer Aufsichtsbehörde bestehen. Die niedrigschwellige Einholung von Expertise ist in einer von Kleinunternehmen geprägten Wirtschaft wichtig, sollen viele Vorschriften nicht auch aus Unwissenheit und Überforderung unbeachtet bleiben. Die Aufsichtsbehörde sollte nach Kommissionsvorstellungen auch eine Liste an Verarbeitungen erstellen, die Gegenstand der vorherigen „Zurateziehung" sind, und hätte diese zu veröffentlichen. Eine Pflicht zur Vorabberatung ist tatsächlich erforderlich, um den bisherigen Vollzugsdefiziten zu begegnen.

Verpflichtende betriebliche Datenschutzbeauftragte: Die verpflichtende Einführung eines betrieblichen Datenschutzbeauftragten in der Privatwirtschaft muss ein Kernstück jeder ernstzunehmenden Datenschutzreform sein. Der weitgehend freie Datenfluss innerhalb der europäischen Wirtschaft legt eine einheitliche EU-Regelung nahe. Das Abgehen von einer verpflichtenden EU-weiten Einführung hin zu einer bloßen Option für den nationalen Gesetzgeber bedeutet, dass die Vereinheitlichung des Datenschutzrechtes in einem überaus zentralen Punkt gescheitert ist. Damit geht die Frage einher, ob der Verordnungscharakter des Rechtsaktes gerechtfertigt ist und nicht einer (Mindestharmonisierungs-) Richtlinie der Vorzug zu geben wäre. Vorschläge, Beauftragte nur in Unternehmen mit mehr als 250 MitarbeiterInnen vorzusehen (EU-Kommission) oder ab 5000 von der Datennutzung Betroffenen (EU-Parlament), gehen am Schutzbedürfnis des Einzelnen vorbei. Für die Bedürfnisse von ArbeitnehmerInnen aber auch KonsumentInnen ist eine obligatorische Einsetzung eines Datenschutzbeaufragten in möglichst vielen Unternehmen (bspw mit mehr als 20 MitarbeiterInnen) doch ein Garant für einen besseren Datenschutzvollzug. Soweit eine EU-weite Einigung völlig außer Reichweite liegt, muss wenigstens eine Melderegisterpflicht bestehen. Eine „weder-noch-Variante" würde den Wirtschaftsinteressen maximal entgegenkommen, ohne aber ein Gleichgewicht mit den legitimen Datenschutzinteressen der Betroffenen herzustellen.

Verpflichtende Datenschutz-TÜVs: Die softe Förderung von Datenschutzzertifizierungen greift zu kurz. In Bezug auf datenschutzsensible Datenanwendungen muss die Zertifizierung verpflichtender Standard sein. Ohne diesen Schritt wird die Verordnung der Maxime, die Datenschutzregeln fit für das 21. Jahrhundert zu machen, nicht gerecht. „Datenschutz-TÜVs" gelten als pragmatische Lösung für Vollzugsprobleme im Datenschutzbereich. Datenverarbeiter sollen demnach sensible Vorhaben auf eigene Kosten durch unabhängige Begutachtungsstellen prüfen lassen. Damit kann Datenschutzkonformität im Großen und Ganzen gewährleistet werden (ob ein Vorhaben als datenschutzrechtlich „heikel" einzustufen ist, sollten die Datenschutzbehörden entscheiden). Die Datenschutzbehörden können nicht Millionen registrierter Datenanwendungen gleichzeitig im Auge behalten und sind derzeit auf Beschwerden angewiesen.

Datenübermittlungen außerhalb der EU: Es ist hinreichend belegt, dass die USA, im europäischen Datenaustausch eine der wichtigsten Datenempfänger, zahllose systematische Datenschutzverletzungen begeht. Das bisherige Genehmigungssystem baut auf Gleichwertigkeitsentscheidungen, Standardvertragsklauseln und „Binding Corporate Rules“ auf, deren Einhaltung aber niemals geprüft wird. Dieses System kann keinesfalls weitergeführt werden. Vor dem Hintergrund des in der Praxis als wertlos geltenden „Safe Harbour-Abkommens“ mit der USA führt letztlich kein Weg daran vorbei, Datentransfers in bestimmte Länder, die über kein gleichwertiges Datenschutzniveau verfügen, zu beschränken.

Abschreckende Verwaltungsstrafen: Nach den ersten Kommissionsplänen sollten die Datenschutzbehörden drakonische Strafen verhängen können: abgestuft bei leichten schuldhaften Verstößen zwischen 100 und 300.000 Euro sowie bei schweren schuldhaften Verstößen zwischen 100.000 Euro und 1.000.000 Euro oder bis zu 5 Prozent des Jahresumsatzes eines Unternehmens. Im offiziellen Entwurf wurde das Vorhaben abgeschwächt: bei erstmaligen „unabsichtlichen“ Verstößen eines Unternehmens mit bis zu 250 Beschäftigten soll der Datennutzer nur verwarnt werden. Abschreckende Strafen sind so gut, wie sie vollzogen werden. Wird die Strafgewalt bspw wegen der Unterfinanzierung der Behörden kaum angewendet, so bleibt die Wirkung einer – wenn auch hohen – Strafdrohung in der Praxis gering.

Behördenkooperation: Die Kooperationsregeln im Falle von Beschwerden an eine Datenschutzbehörde, die mehrere Mitgliedstaaten berühren, sind zu komplex geraten. Mit einer Entscheidung innerhalb angemessener Frist ist dabei kaum zu rechnen. Es ist fraglich, wie sämtliche Äußerungsrechte und Einwandmöglichkeiten für alle beteiligten Behörden und einen europäischen Datenschutzausschuss verfahrensrechtlich zu qualifizieren sind. Die nationalen Datenschutzbehörden werden dadurch auch von nationalen Strukturen und demokratischer Legitimation schrittweise entkoppelt. Die Rechtsschutzmöglichkeiten für die Betroffenen müssen jedenfalls an ihrem Wohnsitzort in jeder Hinsicht gewahrt bleiben.

Detailregeln für spezifische Datennutzungen: Die Anforderungen in Bezug auf die Nutzung von Gesundheitsdaten, ArbeitnehmerInnendaten, soziale Sicherheit usw. sind zum Teil so spezifisch, dass rudimentäre Regeln in einer EU-Verordnung nicht ausreichen. Der nationale Gesetzgeber darf daher – abgehend vom Vollharmonisierungscharakter der Verordnung - nicht daran gehindert werden, in diesen Regelungsbereichen zusätzliche und abweichende - vor allem datenschutzrechtlich - strengere Normen zu erlassen.

6. Verbesserung des Datenschutzes für ArbeitnehmerInnen in Europa

In Österreich aber auch auf EU-Ebene gibt es kaum spezifische Vorschriften, die auf das besondere Schutzbedürfnis der Beschäftigten im Arbeitsverhältnis Bedacht nehmen. Auch der EU-Entwurf zur Datenschutzverordnung geht kaum auf die Besonderheiten von Arbeitsverhältnissen ein. Zum Teil sind sogar Verschlechterungen für die Rechtsdurchsetzung von Betriebsräten und Beschäftigten zu befürchten. Adäquate Datenschutzbestimmungen für ArbeitnehmerInnen und eine effiziente Rechtsdurchsetzung zum Schutz von Beschäftigtendaten im betrieblichen Kontext sollten in Angriff genommen werden.

Dazu zählt:

- Europäische Datenschutzregelungen dürfen die nationalen Arbeitsverfassungen nicht berühren. Sie dürfen diese folglich auch nicht in ihrer Gültigkeit beschränken und bspw bestehende Betriebsratsrechte beschneiden.

- Arbeiterkammern und Gewerkschaften sollen zu den in Datenschutzangelegenheiten (verbands-)klagsberechtigten Einrichtungen gehören.

- Die Stärkung der Position und Bedeutung der Betriebsräte, insbesondere der Konzernbetriebsräte, europäischen und SE-Betriebsräte, indem etwa bei der Zulässigkeit von Datenübermittlungen auf den Abschluss von Betriebsvereinbarungen abgestellt wird statt auf das Vorhandensein einseitig erlassener Arbeitgeberrichtlinien.

- Statt dem One-Stop-Shop - Prinzip muss die Zuständigkeit der nationalen Datenschutzbehörde gewährleistet sein. Außerdem muss ein betrieblicher Datenschutzbeauftragter vor Ort vorhanden sein. Ein Konzerndatenschutzbeauftragter nur am Ort der Hauptniederlassung des Konzerns kann allein den Betriebsräten in diversen Tochterunternehmen nicht als Ansprechpartner dienen.

- Die verpflichtende Bestellung eines betrieblichen Datenschutzbeauftragten ab einer möglichst niedrigen Beschäftigtenanzahl. Generell sind Ausnahmen für kleine und mittlere Unternehmen in Bezug auf den Grundrechtsschutz kritisch zu hinterfragen. Der Schutz der persönlichen Daten der Beschäftigten muss auch in kleinen Betrieben ohne Abstriche gewahrt bleiben.

- Außerdem ist eine Vertretungsbefugnis des Betriebsrats als betriebliche Interessenvertretung seiner ArbeitnehmerInnen in datenschutzrechtlichen Angelegenheiten nötig.

- Erforderlich ist ein Beweisverwertungsverbot für unrechtmäßig erlangte Personaldaten, um den Trend, sich ohne nennenswerte praktische Konsequenzen unfaire Vorteile durch Datenschutzverstöße verschaffen zu können, wirksam zu begegnen.

- Die Wirksamkeit von datenschutzrechtlichen Einwilligungserklärungen im Arbeitsverhältnis ist zu beschränken. Auf Grund des typischen Verhandlungsungleichgewichts im Arbeitsverhältnis erklären sich ArbeitnehmerInnen oft notgedrungen zur Einwilligung bereit und trauen sich aus Angst um ihren Arbeitsplatz in der Folge nicht, diese zu widerrufen. (Auch bei Einwilligungen gem § 10 AVRAG sind auf Grund des typischen Ungleichgewichts erhöhte Anforderungen an die Einwilligung zu stellen, etwa hinsichtlich Schriftlichkeit und Transparenz).

- Im Falle schwerwiegender Datenschutzverletzungen (wie etwa Datenmissbrauch oder –verlust) kann durch eine uneingeschränkte Infopflicht des Auftraggebers die Transparenz (unabhängig von einem - schwer abschätzbaren - drohenden Schadenseintritt bei den Betroffenen) gegenüber Betroffenen und der Datenschutzbehörde verbessert werden.

- Nötig sind Regeln zum externen Whistleblowing. Wenn gewünscht wird, dass Missstände im Betrieb von Beschäftigten der zuständigen Behörde gemeldet werden, so müssen diese vor arbeitsrechtlichen Nachteilen – Kündigungsverbot, Benachteiligungsverbot - geschützt werden.

- Benötigt werden auch internationale Regeln, die sicherstellen, dass Personaldaten in einem rechtlich gesicherten Rahmen grenzüberschreitend transferiert werden und Ansprüche auch im Ausland durchsetzbar sind.

7. Rechtsdurchsetzung

Selbstverantwortung und staatliche Schutzpflichten: Verbraucher- und Datenschützer setzen auf Mahnungen und Warnungen. Medienkompetenz und Risikobewusstsein gegenüber den Gefahren im Internet durch schulische und außerschulische Aufklärung zu vermitteln, ist sinnvoll. Staatlicher Schutz darf sich aber nicht darin erschöpfen. Nicht gläsern und online über den Tisch gezogen zu werden, liegt nicht in der Alleinverantwortung der Betroffenen. Risikovorsorge und Rechtsschutz dürfen nicht privatisiert werden. Der Staat hat auch im Internet für einen ausreichenden Schutz seiner BürgerInnen zu sorgen. InternetnutzerInnen und von Datenschutzverstößen Betroffene dürfen mit ihren Problemen nicht allein gelassen werden. Der grenzüberschreitende Charakter des Internets, die Macht einzelner Internetkonzerne, die Anonymisierungsmöglichkeiten und undurchsichtigen technischen Prozesse begrenzen die Selbstschutzmöglichkeiten der NutzerInnen und damit auch die Selbstverantwortung auf ein bescheidenes Minimum.

Regelbrüche und Vollzugsdefizite: Im Internet wird aus vielen Gründen mitgelesen, Nutzungsspuren gefolgt, Zusammenhänge aus personenbezogenen Einzeldaten ausgewertet, persönliche Daten verändert oder entwendet, eine fremde Identität vorgeschützt und darüber gestritten wird, ob Inhalte zu löschen sind oder im Dienste der Meinungs- und Informationsfreiheit erhalten bleiben sollen. Es wird online in die Irre geführt, betrogen, rechtswidrig geworben und vertrieben, urheberrechtlich Geschütztes rechtswidrig verbreitet, beleidigt, bloßgestellt uvm. Im Vergleich zu den vielen geglückten Aktivitäten im Netz bleibt Cyberkriminalität zwar noch im Rahmen. Sie steigt aber kontinuierlich. Ausstattung und Arbeitsweise von Behörden und Justiz entsprechen nicht mehr den Anforderungen des digitalen Zeitalters. Verstöße im Netz überfordern daher oft den Rechtsstaat. Behörden, Daten- aber auch Verbraucherschützer können der Vielzahl verfolgenswerter Handlungen im Internet kaum etwas entgegensetzen.

Ermittlungen auch bei klein- und besonders großdimensionierten Fällen: Manchmal wird zu Extremen gegriffen: nämlich überschießenden oder ganz unterlassenen Reaktionen. Die Richtlinie zur Vorratsdatenspeicherung gilt zu Recht als Beispiel für einen völlig überzogenen Versuch, öffentliche Sicherheit durch massenhafte Speicherung der Internetverkehrsdaten der Gesamtbevölkerung auf Kosten der Privatsphäre zu gewährleisten. So manches eingestellte Ermittlungsverfahren zeigt andererseits, dass Sachverhalte richtig dimensioniert sein müssen, um zur Rechtsverfolgung zu führen. Der Verfolgung eines Ebay-Betrügers steht der geringe Schadensumfang entgegen. Die Urheber von Phising-Mails sind schwer ausforschbar und jeder einzelne von vielleicht tausenden Streuschäden ist für sich allein betrachtet auch zu gering. Auf der anderen Seite gilt: Internetkonzerne wie Facebook, Google und Co ins Visier zu nehmen, überfordert nicht nur Einzelstaaten, sondern auch die EU-Kommission. Schon allein aus Präventionsgründen verdienen auch Streuschadensfälle eingehende Ermittlungsarbeit. Die Kommission hat, unterstützt von nationalen Behörden und Konsumentenschutzorganisationen, wiederum sicherzustellen, dass auch die global agierenden Internetriesen ihre Dienste EU-rechtskonform gestalten.

Stärkung der Datenschutzbehörde: Die Agentur der Europäischen Union für Grundrechte (FRA) hat 2013 den Zugang zum Recht im Bereich des Datenschutzes analysiert. Aus den Gesprächen mit Opfern von Datenschutzverletzungen geht hervor, dass sich die Mehrzahl an Datenschutzbehörden wendet, um zu verhindern, dass ähnliche Verletzungen erneut geschehen. Eine finanzielle Entschädigung steht dabei nicht im Vordergrund. Nur in Ausnahmefällen beschreiten Opfer den Rechtsweg. Gerichtsverfahren gelten als zu kompliziert, kostspielig und zeitaufwändig. Als problematisch erweisen sich die fehlende Rechtshilfe, Mangel an Datenschutzspezialisten sowie mit zu geringen Ressourcen ausgestatteten Datenschutzbehörden. Darüber hinaus wurde festgestellt, dass zu wenige Informationen über Datenschutzverfahren und Rechtsbehelfe existieren. Viele fanden, dass die Fragmentiertheit und Komplexität des Datenschutzrechtes eine große Hürde für den Zugang zum Recht darstellt. Auch befragte JuristInnen sprechen von einer „Insider-Materie“. So war bereits der unzureichende Zugang zu verständlichen Informationen und kompetenter Beratung eine große Hürde für den Zugang zum Recht. Mitunter war den Befragten unklar, welche Stelle sie mit einem Anliegen ansprechen können. Dieser EU-Befund dürfte weitgehend auch für Österreich gelten.

Ratgeberfunktion: Wegweiser in die Zukunft muss deshalb eine Datenschutzbehörde sein, die als kostenlose Anlaufstelle für Beschwerden weithin bekannt ist, öffentlichkeitswirksam Datenschutzbewusstsein schafft, Missstände aufzeigt und als Kompetenzzentrum zur Weiterentwicklung des Datenschutzes dient. Die Datenschutzbehörde hat zwar derzeit schon eine informelle Ombudsmannfunktion. Jedermann kann sich bei mutmaßlichen Rechtsverstößen von Unternehmen an die Behörde wenden. Die Behörde untersucht den Fall mit den „ihr zur Verfügung stehenden Mitteln und Arbeitskapazitäten“. Gemessen am Beratungsbedarf sind die Ressourcen verschwindend gering. Sie kann bloß eine Empfehlung (die nicht durchsetzbar ist) aussprechen bzw bestimmte andere Maßnahmen setzen (zB Prüfung der Registrierung, Strafanzeige). Ratgeberfunktion und Vollzugsmaßnahmen bei Datenschutzwidrigkeiten von Unternehmen müssen aufgewertet werden.

Mehr Ressourcen: Die personelle Ausstattung der Anfang 2014 neu geschaffenen Datenschutzbehörde ist beklagenswert. Es fehlen Mitarbeiter mit technischer Ausbildung bzw Budgetmittel für den Zukauf von nennenswerten externen Leistungen. Der Internetbenutzer-Verein vibe.at schätzt, dass die österreichische Datenschutzbehörde über rund 45 technische MitarbeiterInnen verfügen müsste, um ihre Aufgaben wie etwa Vorortkontrollen zu erfüllen. Die Funktion einer Ombudsstelle für Ratsuchende ist im Datenschutzgesetz nur rudimentär angelegt. Sie wird nicht zuletzt aufgrund von Ressourcenmangel auch in der Praxis nur eingeschränkt gelebt. Auf Rechtsverletzungen privatwirtschaftlicher Datennutzer (mit Ausnahme von Auskunftsverstößen) kann die Behörde nur mit zahnlosen Empfehlungen reagieren. Von dieser Möglichkeit macht sie in der Praxis auch wenig Gebrauch. Breit angelegte Bewusstseinsbildung und Information der Öffentlichkeit fehlen fast gänzlich.

Überholte Zuständigkeiten: Der Rechtsschutz im Falle von Datenschutzverletzungen ist kompliziert organisiert. Die Datenschutzbehörde erkennt über Beschwerden von Betroffenen, die behaupten, in ihrem Recht auf Auskunft verletzt zu sein (ausgenommen sind die Verwendung von Daten „für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit“). Die Datenschutzbehörde entscheidet außerdem über Beschwerden von Personen, die behaupten, durch Behörden in ihrem Recht auf Geheimhaltung, Richtigstellung oder Löschung verletzt zu sein. Verletzen „privatwirtschaftliche“ Datennutzer (also Unternehmen) andere Datenschutzrechte als das Auskunftsrecht, sind die Betroffenen auf den Zivilrechtsweg verwiesen.

Mit „ortsloser“ Datenverarbeitung in der „Cloud“ löst sich die Vorstellung von einer eindeutigen territorialen Verantwortung von Justiz und Behörden überhaupt auf. Verantwortlichkeiten sind auch deshalb neu zu ordnen.

Niedrigschwelliger Zugang zum Recht: Die Zuständigkeitsverteilung zwischen Behörde und Gerichten ist unzeitgemäß. Im 21.Jahrhundert sind Datennutzungen durch private Unternehmen mindestens ebenso bedeutsam, wenn nicht sogar bedeutsamer, als jene staatlicher Behörden. Die Zahl an Datenschutzbeschwerden gegenüber Unternehmen wächst entsprechend. Die von privatwirtschaftlichen Datenschutzverstößen Betroffenen sind allerdings auf den kostspieligen, unsicheren Zivilrechtsweg verwiesen (Ausnahme: bei der Geltendmachung von Auskunftsverletzungen). Zuständig sind die Landesgerichte für Zivilrechtssachen 1. Instanz am Wohnsitz des Betroffenen. Betroffene schrecken regelmäßig vor einer gerichtlichen Rechtsdurchsetzung zurück. Ziel ist es, den Betroffenen den Zugang zum Recht gegenüber privaten Auftraggebern zu erleichtern. Statt einer zivilgerichtlichen Zuständigkeit mit Anwaltszwang müssen Betroffene ihre Datenschutzansprüche im Bereich der Privatwirtschaft ebenfalls bei der Datenschutzbehörde durchsetzen können. Alternativ kommt auch noch das Außerstreitverfahren vor den Zivilgerichten in Betracht.

Einbeziehung von Stakeholdern in die Behördenarbeit: Bis 2014 wurden Aufsichtsfunktionen und (neben den Zivilgerichten) ein Teil des Rechtsschutzes von der im Bundeskanzleramt eingerichteten Datenschutzkommission als Kollegialorgan (unter richterlichem Vorsitz und unter Einbindung von Mitgliedern, die von den Ländern, der AK und WKÖ nominiert wurden) wahrgenommen. Bescheide der Kommission konnten bei den Gerichtshöfen des öffentlichen Rechts bekämpft werden. Anlässlich einer EUGH-Entscheidung, die der Datenschutzkommission mangelhafte Unabhängigkeit vom Bundeskanzleramt attestierte, und der Reform der Verwaltungsgerichtsbarkeit wurde die Datenschutzbehörde neu gestaltet: sie ist nun monokratisch (Leiter und Stellvertreter) und nicht mehr kollegial organisiert. Damit ist „ein Element deliberativer Entscheidungsfindung verloren gegangen, das weder von Seiten der EU kritisiert noch aufgrund der Verwaltungsgerichtsbarkeit geboten war.“ (Konrad Lachmayer “demokratierechtliche Analyse der Entwicklungsperspektiven des Datenschutzrechtes“ im Auftrag der AK 2014). AK, Gewerkschaften und WKÖ sind nach der Auflösung der Datenschutzkommission zwar in den Vollzug des Datenschutzrechtes als fachkundige Laienrichter in den Senaten des Bundesverwaltungsgerichts eingebunden. Dieses entscheidet allerdings nur über Berufungen gegen Bescheide der Datenschutzbehörde. Da kaum Fälle die neue Berufungsinstanz erreichen, wurde die Partizipationsmöglichkeit der Sozialpartner an der Entscheidungsfindung im Datenschutzbereich erheblich reduziert.

Kontrollen im kollektiven Interesse der ArbeitnehmerInnen und Verbraucher: Nicht nur quantitativ auch qualitativ stützt sich die Entscheidungsfindung nicht mehr auf eine breite Basis an Erfahrungen und Werthaltungen. Weitere Stakeholder sind vom förmlichen Beschwerdeverfahren in erster Instanz aber auch der Mitwirkung am Ombudsmannverfahren, den Vorabgenehmigungen von unternehmerischen Datennutzungen und anderen Kontrollmöglichkeiten im kollektiven Interesse nunmehr gänzlich ausgeschlossen. Dabei haben die letztgenannten Maßnahmen eine erhebliche Tragweite für ArbeitnehmerInnen und VerbraucherInnen.

Ausgewogene Entscheidung über Wertungsfragen: Eine breite Einbindung fachkundiger Stakeholder wäre anzustreben. Die abstrakten Regeln des Datenschutzrechts sind auslegungsbedürftig. Damit ist mehr als in sonstigen Rechtsbereichen ein Spielraum für gesellschaftspolitische Wertungen eröffnet.

Ob bspw „überwiegende berechtigte Interessen“ eine konkrete Datennutzung eines Unternehmens rechtfertigen oder die Vorgangsweise einer Behörde aus Datenschutzsicht „verhältnismäßig“ ist, erfordert nicht nur rechtliche, organisatorische und technische Branchen-Kenntnisse. Neben dem Erfahrungswissen über die näheren Arbeitsumstände, betrieblichen Gegebenheiten, technisch-organisatorischen Abläufe, Wettbewerbs- und Werbepraktiken sind bei der Rechtsgüterabwägung auch individuelle Wertvorstellungen maßgeblich. Eine ausgewogene Entscheidungspraxis würde vor diesem Hintergrund durch ein Kollegialorgan, in dem die Mitglieder mit ihrem unterschiedlichen Erfahrungshintergrund aus verschiedenen Lebenswelten für einen Ausgleich sorgen, begünstigt. Der Rückgriff auf das in einem Kollegialorgan vorhandene horizontale Wissen stellt oft auch eine kostengünstige Alternative zu behördlichen Eigenrecherchen und Auftragsgutachten dar. Bedauerlich ist, dass auch das Vorhaben, einen von fachkundigen Stakeholdern besetzten Beirat einzurichten, der die Datenschutzbehörde unverbindlich berät, nicht weiter verfolgt wurde.

Zusammenwirken von nationalen und EU-Institutionen: Um raschere Ergebnisse zu erzielen, von denen die InternetnutzerInnen in allen Mitgliedstaaten gleichermaßen profitieren, ist eine Bündelung der knappen Ressourcen (für Ermittlungen, Rechtsgutachten, Übersetzungen, Verhandlungen uvm) zweckmäßig. Erst ein gemeinsames Auftreten von Verbraucherverbänden, Datenschutzbehörden und der EU-Kommission schafft jene Verhandlungsmacht, die nötig ist, um die Marktbearbeitungspraktiken weltweit agierende Quasimonopolisten zugunsten der Rechte und Bedürfnisse digitaler NutzerInnen zu beeinflussen. Dieses Zusammenwirken bedarf künftig auch einer institutionalisierten Form. Die Verhandlungsergebnisse dürfen die Mitgliedstaaten allerdings auch nicht daran hindern, einzelne Rechtsfragen auf dem Rechtsweg zu klären.

Grenzüberschreitende Rechtsdurchsetzung erleichtern: Viele Onlineanbieter, die den österreichischen Markt mit unlauteren Praktiken, darunter auch Datenschutzverstößen, bearbeiten, sind außerhalb Österreichs niedergelassen. Anbieter von unseriösen, d.h. im zivilrechtlichen Sinn unlauteren oder im strafrechtlichen Sinn betrügerischen Internetdiensten wenden sich bewusst von anderen Staaten aus gezielt an KonsumentInnen in Österreich. Gesetzwidrige Werbe- und Vertriebsformen (irreführende Webpräsentation, Spam, Verrechnung unverlangter Internetdienste, illegaler Datenhandel uvm) lassen sich überaus kostengünstig online realisieren. Bei Bedarf – etwa Rechtsänderungen oder drohender Rechtsverfolgung – lässt sich die Aktivität ohne viel Aufwand in ein anderes Land verlegen. Damit ist rasches Handeln erforderlich. Ansonsten können Anbieter nicht ausgeforscht werden. Die derzeit häufigste Behördenreaktion: keine. Aus nachvollziehbaren Gründen (chronischer Ressourcenmangel, fehlende Prozesse, die eine reibungslose grenzüberschreitende Zusammenarbeit mit anderen Behörden unterstützen) bleibt die zeit- und kostenaufwändige grenzüberschreitende Rechtsverfolgung in der behördlichen Ermittlungspraxis ein Randphänomen. Der Aufwand ist hoch, die Erfolgsaussichten unsicher. Angesichts einer solchen Bilanz werden Verfahren oft schon eingestellt, bevor sie noch eingeleitet wurden.

Erleichterungen für Konsumentenorganisationen: Unterlassungsentscheidungen in einem Land hindern den Anbieter nicht daran, anderswo auf dieselbe unseriöse Geschäftspraxis zu setzen. Die Zahl grenzüberschreitender Klagen von Konsumentenorganisationen ist entsprechend überschaubar. Auch im Erfolgsfall ist unter Umständen wenig gewonnen. Ein schönes Beispiel dafür sind die Klagsanstrengungen des deutschen Verbraucherschutzverbandes VZBV gegenüber Facebooks lockerem Umgang mit europäischem Konsumenten- und Datenschutzrecht. Nach zweijähriger Prozessführung ist geklärt, dass für den Social-Media-Monopolisten deutsches und nicht irisches Recht gilt.

Das Kammergericht Berlin erklärte zudem einige Geschäftsklauseln für unwirksam und forderte klare Angaben zur Funktion des Freundefinders. Die Klauseln und Features haben sich aber zwischenzeitig schon mehrfach und maßgeblich geändert. Die Wirkung des Urteils erstreckt sich kraft des Territorialitätsprinzips auch keineswegs auf alle EU-Länder, obwohl die Entscheidung weitgehend auf EU-Recht basiert. Facebook setzt in Europa weiter unbeirrt auf seine vertraglichen Gestaltungswünsche und fügt nur, soweit notwendig, zB partielle Anwendungsausschlüsse für deutsche NutzerInnen ein. Weder Datenschützer, Verbraucherorganisationen noch Gerichte halten bei diesem Tempo mit. Der Erfolg steht oft in keinem Verhältnis zum Aufwand.

Unbedingt notwendig ist daher

- **Ein EU-weites Firmenbuch:** Auf EU-Ebene ist dafür zu sorgen, dass in allen Mitgliedsländern allgemein abrufbare Firmenregister eingerichtet sind. Jedermann innerhalb der EU soll sie kostenlos nutzen können. Für ihre Aktualität sind die Mitgliedstaaten verantwortlich. Diese Transparenzmaßnahme ist erforderlich in Hinblick auf die hohen Mobilität von Internetdiensten, die Zunahme grenzüberschreitender rechtswidriger Praktiken und der allzu häufigen Missachtung der Anbieterpflicht, den Firmennamen und die genaue Sitzadresse offenzulegen.

- **Eine Reform der Verbindungsstellen**: Die Funktion und Effizienz der Verbindungsstellen nach der E-Commerce-Richtlinie sind zu überdenken. Diese hätten sicherzustellen, dass Mängel von Webseiten rasch beseitigt werden. Das Netz an Verbindungsstellen hat wenig Relevanz, da nicht alle Mitgliedstaaten dieser Pflicht mit der nötigen Ernsthaftigkeit nachkommen.

- **Drittstaatenkooperationen:** Drittstaaten, die zur Umgehung von EU-Standards als Ausgangspunkt rechtswidriger Handlungen gewählt werden, sind stärker in die Behördenzusammenarbeit mit einzubeziehen.

- **Anstrengungen der EU-Kommission:** Die EU-Kommission hat Verhandlungen über Verhaltensregeln mit den Internet-Riesen Google, Facebook usw. aufzunehmen. Sie verfügt am ehesten über die für eine Durchsetzung europäischen Rechts nötige Verhandlungsmacht.

- **Kapazitäten aufzubauen:** die Ressourcen bei Behörden, Gerichten und Verbrauchereinrichtungen sind den enorm hohen Anforderungen entsprechend auszubauen.

8. Verhältnis zu den USA

Aussetzen von Safe Harbor: Die Datenschutzrichtlinie verbietet, personenbezogene Daten aus der EU in Staaten zu übermitteln, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, die auf keine Regeln verweisen kann, die jenen der EU entsprechen. US-Unternehmen können zwar dem Safe Harbor beitreten und sich dazu auf einer Liste des US-Handelsministeriums eintragen lassen. Sie verpflichten sich damit, einige Datenschutzgrundsätze zu beachten. Im Jahr 2000 hat die EU entschieden, dass bei Unternehmen, die dem Safe-Harbor-System beigetreten sind, ausreichender Schutz gewährleistet sei.

Im Zuge des NSA-Skandals forderte das EU-Parlament die Aussetzung dieses Abkommens. Die EU-Kommission reagierte darauf mit der Absichtserklärung, das Abkommen „konsolidieren“ zu wollen. Da es aber den USA an einem adäquaten Datenschutz mangelt, wäre eine Aussetzung der Safe Harbor Entscheidung die einzige rechtskonforme Lösung.

An der EU-Grundrechtstradition festhalten: Die EU-Kommission wird nicht umhin kommen, die Datenschutz-Verhandlungen mit den USA zu intensivieren. Dabei darf sie von der europäischen Tradition eines vergleichsweise strengeren Datenschutzes nicht abrücken. Gerd Billen, Staatssekretär des deutschen Verbraucherministeriums, verweist darauf, dass „über Server von US-Unternehmen vier der fünf populärsten Suchmaschinen laufen. Alleine Google hat in Deutschland einen Marktanteil von über 95 Prozent. Drei der sieben populärsten E-Mail-Dienste speichern unsere Daten auf US-Servern“. Der Schutz europäischer BürgerInnen hängt folglich nicht allein von der Rechtstreue europäischer Datenverarbeiter ab. Solange Europa nicht mit erfolgreichen Alternativangeboten zu den US-Diensten aufwarten kann, bleibt nur ein Weg: die EU muss sich für eine Akzeptanz europäischen Datenschutzes bei den US-Internetkonzernen und ein Vollstreckungsabkommen mit der EU einsetzen.

Bei TTIP hohe Priorität für strikten Datenschutz: Im Zuge der TTIP-Verhandlungen zu einem Freihandelsabkommen zwischen den USA und der EU darf die EU den Konflikt zwischen verschiedenen Datenschutztraditionen nicht scheuen. Der Datenverkehr zwischen der EU und den USA hat schließlich enormen Umfang. Abseits von Google-Daten ist vor allem auch an das SWIFT-Abkommen zu denken. Dieses ermöglicht die Abwicklung des Datenaustauschs zwischen europäischen Kreditinstituten – etwa in Bezug auf Kundendaten bei Standardüberweisungen – durch einen US-Dienstleister. Das EU-Parlament plädierte im Sog der NSA-Spionageaffäre auch für eine sofortige Beendigung der SWIFT-Kooperation. Ein gemeinsames Freihandelsabkommen muss deshalb auch dem Datenschutz einen ungleich höheren Stellenwert einräumen als bisher.

Kooperation zwischen den Verbraucherverbänden, Datenschutzbehörden und der europäischen Kommission: Digitale Rechtsdurchsetzung insbesondere Datenschutzanliegen stößt derzeit in Bezug auf „Over-the-Top-Player“ wie Google, Apple, Facebook usw rasch an Grenzen. Klagen wegen unlauteren Wettbewerbs, Datenschutzverstößen und rechtswidriger AGBs gehen ins Leere, weil die rechtliche Klärung meist Jahre in Anspruch nimmt und Dienste oder Vertragsinhalte sich zwischenzeitig erheblich geändert haben. Entscheidungen haben außerdem nur territoriale Wirkung (gelten mit anderen Worten nicht in allen Mitgliedstaaten). Die belangten Konzerne reagieren darauf auch oft mit einem kompletten Rückzug (des jeweiligen Produktes; siehe zB Google Street View) aus (nicht bedeutsamen) Märkten. Eine Reaktion, die nicht im Sinne der Verbraucher ist, da der grundsätzliche Mehrwert der Dienste unstrittig ist.

Eine eigene Suchmaschine für Europa: Um nach der Eingangsbemerkung nochmals aus Frank Schirrmachers Rede vom deutschen Verbrauchertag 2013 zu zitieren: *„Wir alle suchen nach einer Vision für Europa. Wir sehen, dass in der Informationsökonomie zusammen mit der Globalisierung zwei Supersysteme entstehen: die USA auf der einen Seite, auf der anderen Seite Asien, vor allen Dingen China. Europa dagegen sucht noch nach einer eigenen Aufgabe, Vision und Identität. Wer das Silicon Valley bewundert, muss dabei bedenken, dass es über Jahrzehnte staatlich subventioniert war – und zwar bis in die 1980er-Jahre. Was da passiert ist, ist also nicht nur ein Ergebnis des Entrepreneurships.*

Wir müssen uns fragen, ob wir uns weiterhin von Systemen abhängig machen wollen, die ausschließlich aus den USA kommen. Oder ob Europa nicht auch mit Hilfe staatlicher Subventionen eigene Suchmaschinen aufbaut – oder eigene soziale Netzwerke, die dann den Vorteil hätten, dass sie neu konstruiert werden könnten."

Datenschutz und digitale Nutzerrechte muss auch Eingang in die Förderpolitik finden. Im Gefolge der NSA-Spionagedebatte kam von vielen Seiten der Wunsch, Europa möge sich mit eigener technischer Infrastruktur stärker von den USA emanzipieren. Von außereuropäischen digitalen Medien, Geräten und der Infrastruktur langfristig unabhängiger zu werden, ist überaus zweckmäßig. Andernfalls bleiben wir in Bezug auf die Gestaltung und Durchsetzung von digitalen Nutzerrechten wenig souverän.

9. Zusätzlicher Gestaltungsbedarf für die digitale Welt

Stopp der Privatisierung der Rechtssetzung: Das Knowhow in Bezug auf technische Innovationen beschränkt sich oft auf wenige Stakeholder. Sie sind meist nicht repräsentativ für die Gesamtbevölkerung und verfolgen oft Partikularinteressen. Dennoch kommt ihnen großes Gewicht zu, etwa wenn nationale oder EU-Behörden beraten werden wollen und staatliche Entscheidungen oft auf Beratungsgremien ausgelagert werden, die staatlich nicht ausreichend legitimiert sind. In Bezug auf den Datenschutz und digitale Nutzungsrechte berührt das bspw den Bereich der technischen Normung von Geräten, Sicherheitsmaßnahmen usw. Regulierung und Gesetzgeber ordnen an, dass datenschutzsensible Anwendungen zB Datensicherheitsmaßnahmen auf dem „Stand der Technik" zu halten haben oder Schutzmaßnahmen zu treffen sind, „soweit technisch machbar und wirtschaftlich zumutbar". Die Beurteilung dieser Gemeinplätze wird anderen überlassen. Gesetzgeber bzw Behörden müssen die konkreten Anforderungen an die Datensicherheit jeweils selbst festlegen.

Wunschsperren für automatische Suchmaschinenzugriffe auf Websites mit Augenmaß:
Der Europäische Gerichtshof hat 2014 Google verpflichtet, Suchergebnisse auf Wunsch eines Betroffenen zu löschen. Ein Spanier hatte Google dazu aufgefordert. Bei Eingabe seines Namens schien nämlich die amtliche Mitteilung einer mehr als ein Jahrzehnt zurückliegenden Zwangsversteigerung seines Hauses im Online-Archiv einer Zeitung auf. Google musste dem Urteil des EUGH folgend die Verknüpfung zu diesem Artikel aus seinen Suchlisten entfernen. Denn die Suchmaschine erleichtere den Zugang und die Verbreitung von Informationen in einer Weise, wie es die Zeitungsmeldung gar nicht vermag. Die Auffindbarkeit des Links über die Suchmaschine kann daher, so der EUGH, einen stärkeren Grundrechtseingriff darstellen als eine Webseiten-Info. Datenschutzinteressen gingen dem Interesse der NutzerInnen an einem freien Informationszugang nach Art 11 Grundrechtecharta dabei in der Regel vor. Auszunehmen davon sind jedenfalls Personen, an denen ein öffentliches Interesse besteht.

Mit dieser allgemeinen Wertung handelte sich der EUGH bei Kritikern den Vorwurf ein, Zensur zu begünstigen. Das Recht auf Vergessen wächst sich bei Google auch zum Problem aus: zehntausenden individuellen Löschanträgen stehen Aufrufe gegenüber, die Pressefreiheit zu schützen. Unter welchen Umständen soll ein verantwortlicher Betreiber nun löschen? Fragen dieser Größenordnung können nicht Suchmaschinenbetreibern überlassen werden. Sonst läuft man Gefahr, dass in der Praxis Willkür herrscht. So beklagte etwa ein Journalist des britischen Guardian, Google habe Links zu kritischen Artikeln über einen Schiedsrichter aus dem Suchindex entfernt. Google soll die Löschung rückgängig gemacht haben. Der EUGH hat jedenfalls ausgeführt, dass für ein erfolgreiches Löschbegehren kein Schadensnachweis nötig sei. Es reicht, wenn die Daten aufgrund der verstrichenen Zeit nicht mehr erforderlich sind.

Es ist daher zu klären:

- welche Kriterien geben im Zweifelsfall den Ausschlag für die Durchführung bzw Verweigerung einer Löschung (der Indizierung durch Suchmaschinenbetreiber, aber auch von Internetinhalten, die Hostprovider speichern).

- Angesichts massenhafter Löschwünsche sollten Befürworter wie Gegner einer konkreten Löschung nicht nur auf den kostspieligen, riskanten Zivilrechtsweg verwiesen werden. Die Einrichtung einer unabhängigen Schlichtungsstelle wäre eine Hilfestellung.

- Google löscht nur Treffer auf den europäischen Seiten. Außereuropäische IP-Adressen haben nach wie vor Zugriff auf eine ungefilterte Linkliste. Ob dies angemessen ist, ist zu klären.

- **Transparente und faire Suchmaschinenrankings:** Google mit über 1 Milliarde monatlichen Besuchern ist weitgehend konkurrenzlos. Andere Suchmaschinen wie Bing und Yahoo! Search rangieren im Vergleich unter ferner liefen. Die Suchmaschinenanbieter bemühen sich um den Eindruck, dass ihre Ergebnisreihung mit Hilfe unbestechlicher Suchalgorithmen zustande käme. Welche Website passt besser zu einer Suchanfrage und welche ist bedeutsamer, weil viele Drittseitenlinks darauf verweisen. Darüber hinaus sind die Faktoren, nach denen eine Website von Suchmaschinen gereiht wird, schwer durchschaubar. Google musste sich den Vorwurf gefallen lassen, dass eigene Angebote und Markenangebote besonders oft an Top-Positionen zu finden sind. Um angesichts Googles Marktdominanz fairen Wettbewerb sicherzustellen, sollte die Suchmaschinenlogik transparenter sein. Die Auswahlkriterien nach eigenen Bedürfnissen verändern zu können, wäre im Interesse der NutzerInnen. Techniken, die über eine Suchmaschinenoptimierung hinausgehen, und manipulativ sind (zB durch Seiten, die zwecks besseren Rankings nur für die Suchmaschine bestimmt sind), müssen zurückgedrängt werden.

Datenschutzvorgaben für die Nutzung von Sozialen Netzwerken: Web 2.0-Technologien laden im Internet „zum Mitmachen“ ein. Praktisch jeder kann praktisch alles ohne Spezialwissen mit einem homepageartigen Profil im Internet sichtbar machen. Soziale Netzwerke setzen die Veröffentlichung von Informationen zur eigenen Person voraus. Ihre Nutzung befindet sich daher automatisch in einem Spannungsfeld zwischen öffentlicher Präsentation und dem Schutz der Privatsphäre. Etwas, worauf wir heute stolz sind, kann in einigen Jahren unangenehm sein. Einmal veröffentlichte Daten sind weltweit zugänglich, schnell vervielfältigt und oft nicht mehr zu entfernen. Inhalte sind nicht nur für FreundInnen zugänglich, sondern theoretisch auch für alle anderen InternetnutzerInnen auf der Welt. Private Informationen können jederzeit für andere Absichten missbraucht werden. Der erste Eindruck zählt auch bei Personalbüros, die mithilfe von Online-Profilen Interessen und die politische Meinung recherchieren können. Das virtuelle Bild einer Person kann einseitig oder schlicht falsch sein. Nicht alles ist, wie es scheint: sich als jemand anderer auszugeben bzw etwas vorzuspielen, ist im Web einfach. Für NutzerInnen ist es unumgänglich, sich der Risiken einer allzu großen „Freizügigkeit“ im Internet bewusst zu werden und kritisch mit persönlichen Daten umzugehen. Betreiber sind gefordert, Einstellungen zum Schutz der Privatsphäre anzubieten, diese strikt voreinzustellen und Datenschutz-Bestimmungen verlässlich einzuhalten.

Werbung in Sozialen Netzwerken: Die meisten Plattformen finanzieren sich über zielgerichtete Werbung. Dieses Geschäftsmodell lässt sich mit der Idee der Datensparsamkeit schwer in Einklang bringen. Entsprechend großzügig sind auch die Zugriffsrechte der Betreiber auf Daten ihrer NutzerInnen.

Versteckte, sich häufig ändernde und unverständlich formulierte Datenschutzerklärungen überfordern NutzerInnen. Problematisch ist auch, dass die Plattformen Löschwünschen nur teilweise nachkommen. Benutzerkonten werden deaktiviert, die Daten aber physisch nicht vollständig gelöscht. Immer wieder treten Sicherheitslücken auf, durch die der unerlaubte Zugriff Dritter auf NutzerInnen-Daten möglich wird. Die möglichen Folgen: E-Mail-Adressen und andere private Daten werden zB für Spam missbraucht, Fotoalben widerrechtlich auf Tauschbörsen zum Download angeboten oder NutzerInnen-Profile weiterverkauft.

Verbindliche Regeln sind deshalb nötig, zB:

- Die Voreinstellung von Zugriffsmöglichkeiten – zB auf das Nutzerprofil – muss möglichst restriktiv sein
- Persönliche Daten sind von Suchmaschinenzugriffen auszunehmen; eine Suchmaschinenindizierung darf nur mit ausdrücklicher Einwilligung vorgenommen werden.

- Zustimmungsklauseln müssen den gesetzlichen Anforderungen besser entsprechen (Transparenz, Verständlichkeit, Sichtbarkeit, Freiwilligkeit, Erteilung für den konkreten Einzelfall). Datenfreigaben sollten von den NutzerInnen eigens aktiv angehakt werden müssen. Über neue Funktionen sind NutzerInnen gut sichtbar aufzuklären. Ihre Freischaltung setzt ebenfalls eine ausdrückliche Einwilligung voraus. Auch Anwendungen Dritter dürfen nur mit ausdrücklicher Einwilligung der Nutzer auf die Daten zugreifen.
- Minderjährige sind besonders zu schützen

- Informationen müssen verständlich formuliert sein
- Nutzerdaten müssen nach Widerruf von freiwilligen Zustimmungen zur Datennutzung und der Beendigung der Dienstnutzung vollständig gelöscht werden.

- Bei selbstgenerierten Beiträgen muss ein „Recht auf Vergessen“ bestehen. Den Betreibern stehen keine umfassenden Nutzungsrechte an den Inhalten der Nutzer zu.

- Bei Löschwünschen hinsichtlich fremdgenerierter Informationen mit Personenbezug muss der Plattformbetreiber die Interessen (Datenschutz, Informationsfreiheit uä) gegeneinander abwägen und dem Betroffenen eine begründete Stellungnahme über seine Entscheidung zukommen lassen.

- Im Missbrauchsfall (zB Identitätsdiebstählen) muss der Betreiber rasch auf Sperrmeldungen reagieren.

Stopp für rechtswidrige Tracking-Methoden: Die Regulierung des Einsatzes von technischen Werkzeugen, mit deren Hilfe das Nutzerverhalten im Netz nachverfolgt werden kann, muss wirksam und praxisnah sein. Die Anstrengungen zur Eindämmung des rechtswidrigen Ausspionierens des Surfverhaltens sind zu vergrößern. Der Rechtsschutzbedarf bezog sich bislang vorrangig auf die massenhafte Verbreitung unerlaubt eingesetzter Cookies - kleiner Softwareprogramme (zB wenn sie verdeckt eingesetzt werden, eine Datenverwertung für andere als die ausgewiesenen Zwecke vorgenommen wird, bei übermäßiger Speicherdauer und unzulässiger Datenweitergabe an Dritte). Aber auch der Einsatz von Deep Package Inspection, einem Verfahren mit dem Datenpakete im Internet überwacht und gefiltert werden, braucht einschränkende Regeln. Inzwischen sind neue Technologien (zB Canvas Fingerprinting) hinzugekommen, die ebenso genaue Nutzerprofile über Surfgewohnheiten ermöglichen und für den Internetnutzer über die Sicherheitseinstellungen seines Browsers kaum erkenn- und blockierbar sind.

Grenzen für die Nutzung von Big Data Analysen und Prognosen: Wie alt sind Sie? Wo wohnen Sie? Wie viel verdienen Sie? Welche Gesundheitsbeschwerden haben Sie? Daten werden zu den unterschiedlichsten Zwecken verarbeitet. Werden Daten aus verschiedenen Datenbeständen zusammengefügt, entsteht ein sehr genaues Bild mit Informationen über uns, die wir so nie preisgeben würden. Voraussetzung für die Anwendung von Datenanalyse-Techniken ist natürlich, den Rohstoff „Daten“ zunächst umfassend zusammen zu tragen. Das Anlegen solcher Datenpools wird gerne als "Data Warehousing" bezeichnet. Im Data Warehouse werden die Daten der einzelnen Abteilungen eines Unternehmens mit zugekauften Daten angereichert, losgelöst von ihrer ursprünglichen Verwendung gespeichert und für Data Mining Analysen zugänglich gemacht. Neue Methoden der Datenanalyse sollen ähnlich der Rohstoffgewinnung im Bergbau verborgene Schätze in den Daten heben. Data Mining-Techniken versuchen nützliche Muster und Beziehungen zwischen Einzeldaten in großen Datenbeständen zu ermitteln. Unternehmenskonzentrationen und Outsourcing begünstigen den Zugriff auf große Datenmengen.

Gearbeitet wird mit Assoziationen (bspw die Analyse von Warenkörben, etwa zur Bestimmung der Häufigkeit, mit der unterschiedliche Produkte gemeinsam gekauft werden), Sequenzen (erfassen die Regelmäßigkeiten im zeitlichen Ablauf, bspw die Anschaffung von Haushaltsgeräten nach dem Bezug einer neuen Wohnung), Klassifikationen (zB Zuordnen zu unterschiedlichen Kreditwürdigkeitsklassen), Cluster (bspw die Definition einer Kundengruppe mit besonders hoher Neigung zum Anbieterwechsel) und Prognosen (zukunftsgerichtete Verhaltensannahmen). Das Wissen über Personen dient nicht nur dazu, Waren und Dienste den Bedürfnissen der Konsumenten entsprechend zu optimieren. Datenanalysen werden immer öfter angestellt, um das Verhalten der Konsumenten im Sinne des Unternehmens zu steuern und unerwünschte Beziehungen auszusondern. Wenn sich über den Dienst „Google Trends“ anzeigen lässt, wie oft Nutzer innerhalb eines Zeitintervalls nach einem bestimmten Begriff gesucht haben, können damit nützliche Prognosen erstellt werden. Etwa der baldige Ausbruch einer Grippewelle, wenn zeitgleich viele NutzerInnen im Netz nach Symptomen und Behandlungsvorschlägen suchen.

Es gibt eine Fülle an problematischen Seiten, die bereits 2002 von der Akademie der Wissenschaften für die AK aufgearbeitet wurden: Daten werden für zukünftige Auswertungen mit unbekannten Zielen gehortet. Das Prinzip der strikten Zweckbindung in der Datenverarbeitung wird dabei missachtet. Auch Datendepots, die sich jederzeit für neue Ziele reaktivieren lassen, widersprechen dem Datenschutzgedanken. Einwilligungen zur Datenverarbeitung werden durch den Einsatz von Data Mining Verfahren zu Generalvollmachten. Die Einsatzmöglichkeiten sind für die Betroffenen nicht mehr einschätzbar. Die Missbrauchsgefahr wächst. Ob die Aufdeckung von verborgenen und unbekannten Beziehungen ein eindeutiger Zweck sein kann, ist mehr als fraglich. Unklar ist auch, ob Zustimmungen von Betroffenen zur Analyse ihrer Daten im Rahmen von Data Mining Prozeduren überhaupt rechtlich wirksam sein können. Problematisch ist die Vermengung von Fakten mit Resultaten von Datenanalyseverfahren. Durch die Zusammenfassung der beiden Arten von Daten in persönlichen Profilen wird ein weiteres Datenschutzprinzip gebrochen, nämlich das Prinzip der Datenqualität. Das Bild über eine Person kann so erheblich verfälscht sein. Mit diesem Verfahren kann auch – etwa im öffentlichen Sicherheitsinteresse - normabweichendes Verhalten einzelner Personen erkannt werden.

Eine Entwicklung, vor der schon 1983 das deutsche Bundesverfassungsgericht in einer Grundsatzentscheidung (Volkszählungsurteil) gewarnt hat: Wer nicht weiß oder beeinflussen kann, welche Informationen bezüglich seines Verhaltens gespeichert werden, passe aus Vorsicht sein Verhalten an. Dies beeinträchtigt nicht nur die individuelle Handlungsfreiheit, sondern auch das Gemeinwohl, da ein freiheitlich demokratisches Gemeinwesen der selbstbestimmten Mitwirkung seiner Bürger bedarf.

Es besteht also Handlungsbedarf, zB:

- Auch im Bereich datenbasierter Prognostik zielen Verbesserungsmaßnahmen vor allem auf eine effektivere Durchsetzung geltenden Datenschutzrechts ab.

- Viele wertvolle Aussagen lassen sich auch auf Basis anonymisierter Daten treffen.

- Herkömmlicher Datenschutz ist um ein Verbot der Diskriminierung durch Bewertungsprozesse zu ergänzen und Rechtslücken in Bezug auf die Zweckbindung von Daten zu schließen.

- Die zeitliche Dimension lässt sich durch ein Verbot längerfristiger Speicherung personenbezogener Daten einschränken. Die Menge an Daten, die Data Mining Analysen zugeführt werden kann, hängt von den Möglichkeiten ab, auf Fremddaten zuzugreifen, und vom Umfang der Geschäftstätigkeit des betroffenen Unternehmens. Global tätige Internetkonzerne aber auch US-Direktwerbefirmen wie zB Acxiom (samt ihren europäischen Ablegern), die laut New York Times auf mehr als 23.000 Servern Infos über 500 Millionen Personen zusammenstellt, sind Kontrollen zu unterziehen. Darauf muss sich die EU gegenüber den USA verständigen. Rechtlich und organisatorisch muss sichergestellt sein, dass keine unternehmensübergreifenden Datenauswertungen stattfinden können.

Ausübungsregeln für Scoring: Daten dienen immer mehr dazu, künftige Lebensumstände von Personen vorherzusagen. Bonitätsbewertungen durch weitgehend automatisierte Scorings entscheiden zB immer öfter, ob KonsumentInnen als Vertragspartner akzeptiert werden. Personen werden dadurch als Risiko- und Kostenfaktor wahrgenommen und die einzelnen Risikoprofile mit großem Aufwand verfeinert. Anstrengungen zur Beseitigung von Unsicherheit und sozialen Ungleichheiten treten dagegen in den Hintergrund. Rechtspolitik muss sich ernsthaft mit den Methoden des Scorings und seinen sozialen Folgen auseinandersetzen. Im Regierungsübereinkommen wurden Regeln fürs Scoring - vorzugsweise im Datenschutzgesetz – in Aussicht gestellt.

Aktuell kommen vor allem Bonitäts-Checks zum Zweck der Berechnung eines Zahlungsausfalls zum Einsatz. Sie sind intransparent. Betroffene wissen oft nicht einmal, dass sie durchleuchtet werden, geschweige denn, was an persönlichen Daten gesammelt wird. Die Menge der für Scoring-Zwecke durchkämmbaren Daten nimmt durch die Digitalisierung schnell zu. Nicht nur die Zahlungsmoral eines Konsumenten in der Vergangenheit steht im Fokus. Immer öfter geht es um Blicke in die Zukunft, wie er/sie künftig dasteht: Job, Familienstand, ... Solche statistischen Methoden führen zu ethischen und rechtlichen Problemen – denn viele Facetten sozialer Wirklichkeit lassen sich nicht in Zahlen abbilden.

Rating (Einstufung) und Scoring (Punktevergabe) sind mathematische Verfahren zur Bewertung menschlichen Verhaltens. Mit Hilfe von Fakten, allgemeinen Erfahrungen und statistischen Werten wird etwa die Wahrscheinlichkeit berechnet, mit der ein Kunde seine Zahlungspflichten erfüllen bzw verletzen wird: Kann sich der/die Konsument/in den Vertragsabschluss leisten, wird er/sie pünktlich zahlen und dem Unternehmen lange treu bleiben?

Alles, was man über den potenziellen Vertragspartner weiß oder aufgrund statistischer Zuschreibungen auch nur zu wissen glaubt, fließt in einen numerischen Wert (den Score) und dann in die unternehmerische Entscheidung ein: bei der Zusage oder Verweigerung eines Vertrages, bei der Festlegung von Konditionen und bei eventuellen Preis- oder Zinsverhandlungen. Minuspunkte bringen häufige Umzüge – sie gelten als Indiz für einen unsteten Lebenswandel. Junge, ledige Personen und solche, die erst seit kurzer Zeit eine Arbeit haben oder in einer Miet- statt Eigentumswohnung leben, werden tendenziell schlechter eingestuft. Scheidungen, unterhaltspflichtige Kinder, Karenzgeldempfang oder Saison-Arbeit beeinflussen die Bonitätsbewertung ebenso negativ.

Klar ist, dass eine Kreditvergabe nicht ohne Sicherheiten und Überprüfungen ablaufen kann. So gibt es für Banken auch die Sorgfaltspflicht nach dem Bankwesen- und Verbraucherkreditgesetz, die Bonität ihrer KreditnehmerInnen zu prüfen. Inzwischen greift aber selbst der Onlinehandel auf Scorings zurück. Hinzu kommt der internationale Trend, Scoringmodelle mit Informationen anzureichern, die absolut nicht für Bonitätsbewertungen gedacht sind (etwa Einträge in Facebook). Auch von den Handy-Standortdaten eines Konsumenten kann auf dessen Lebenswandel geschlossen werden (Aufenthaltsorte, Beziehungsverhalten, Nachtruhe). Das Schürfen in Datenbeständen wie in Sozialen Netzwerken hilft bei der Prognose, ob in drei Jahren noch ein Arbeitsplatz und gemeinsamer Ehehaushalt vorhanden ist. Solche Faktoren beeinflussen wiederum die Wahrscheinlichkeit, dass eine Schuld zurückgezahlt werden kann. Ist in der Praxis schon die Rückschau fehleranfällig, so gilt das für Prognosen umso mehr. Dabei werden mittels statistischen Prozessen inzwischen ganze Bevölkerungsgruppen klassifiziert und (aus)sortiert.

Regulierungsdefizit: Angesichts der einschneidenden Bedeutung von Scoring-Entscheidungen für die Betroffenen ist das Ausmaß der Regulierung absolut dürftig. Es braucht mehr Schutz:

- **Nur bestimmte Datenarten verwenden:** Wirtschaftsauskunfteien dürfen nach der Gewerbeordnung Angaben über Kreditverhältnisse und Zahlungsfähigkeit eines Schuldners verwenden. Verboten ist die Erteilung von Auskünften über private Verhältnisse, die mit der Kreditwürdigkeit in keinem Zusammenhang stehen. Völlig unklar ist, wie weit dieser Zusammenhang in der Praxis geht. Viele höchstpersönliche, private und sensible Informationen über das Leben und die Gesundheit können der Vorhersage der Zahlungsausfallwahrscheinlichkeit dienen. Die Datensammlung muss sich auf unmittelbar bonitätsrelevante Daten beschränken. Das wären im Prinzip die Einkommenssituation und die zu erwartenden Ausgaben. Zudem dürfen Daten, die zweckfremd erhoben wurden, nicht in Scoring-Modellen verarbeitet werden. Die Daten dürfen weder alt noch diskriminierend sein.

- **Mehr Klarheit für Betroffene**: Möchte ein Verbraucher Auskunft über die zu seiner Person in einer Bonitätsdatenbank gespeicherten Daten, so ist ihm der Dateninhalt zwar vollständig und verständlich mitzuteilen (Codes und Abkürzungen sind etwa zu erläutern). Bei automatisierten Entscheidungsabläufen sollten neben den Kriterien für die Bonitätsbeurteilung aber auch ihr Gewicht bei der Gesamtbeurteilung offengelegt werden, damit der Ablehnungsgrund für den Betroffenen nachvollziehbar wird. Die Datennutzer berufen sich dabei aber gerne auf Geschäfts- und Betriebsgeheimnisse.

- **Aktualisierung:** Die Datenschutzbehörde hat im Zusammenhang mit Datenbanken des KSV festgehalten, dass in die Kleinkreditevidenz eingetragene Zahlungsanstände mindestens einmal jährlich, alle anderen Daten spätestens alle drei Jahre auf ihre Richtigkeit überprüft werden müssen. Verbraucher sollten von Datenabfragen informiert werden, um die Aktualität der Angaben prüfen zu können.

- **Geringere Speicherdauer**: Betroffene können gegen die Aufnahme in eine Bonitäts-Datenbank ohne Begründung Widerspruch erheben, dann nämlich, wenn es sich um eine öffentlich zugängliche Datei handelt und die Aufnahme nicht gesetzlich angeordnet ist. Die Daten sind dann binnen acht Wochen zu löschen. Seit Inkrafttreten des Verbraucherkreditgesetzes 2010 gibt es aber eine wesentliche Ausnahme: Ein begründungsloser Löschungsanspruch besteht nicht mehr bei den als Informationsverbundsystem organisierten Datenbanken der Kreditinstitute. Die Löschung lässt sich aber selbstverständlich weiterhin durchsetzen, soweit Daten unrichtig sind, aus rechtswidrigen Quellen stammen, Infopflichten oder besondere schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt wurden. Als Richtschnur für die Aufbewahrungsdauer der Daten dient ein Bescheid der Datenschutzbehörde zur Konsumentenkreditevidenz: Bei Zahlungsanständen ist spätestens fünf Jahre nach vollständiger Bezahlung der Schuld, ansonsten sieben Jahre nach Schuldtilgung zu löschen. Die Höchstspeicherdauer sollte festgelegt und dabei verkürzt werden.

- **Unverhältnismäßige Abwälzung des Unternehmerrisikos:** Automatisierte Bonitäts-Checks bei kleinen Summen und allgemeinen Unternehmensrisiken sind überschießend und einzuschränken. Es ist klar, dass die Kreditvergabe Sicherheiten benötigt. Bedenklich ist aber der Trend zur Mehrfachabsicherung, bei der etwa ein Bonitätsprofil erstellt, eine Lebensversicherung vinkuliert und noch eine Kreditausfallversicherung zu Lasten des Kreditnehmers abgeschlossen werden. Die Bank würde sich dreifach absichern, ohne dass erkennbar ist, worin das unternehmerische Risiko der Bank bestünde, für das eine KreditnehmerIn ja auch zu zahlen hat.

- **Zweifelhafte Qualität des Scorings**: Ohne ständige Prüfung kann das Scoring-Verfahren schnell zu falschen Prognosen führen. Eine deutsche Studie aus 2009 analysierte die Datenqualität von Wirtschaftsauskunfteien über Selbstauskünfte von Testpersonen. Das Ergebnis zeigt: Rund 45 Prozent der Auskünfte weisen fehlerhafte, unvollständige oder falsche Eintragungen auf. Die verschiedenen Bewertungs- und Berechnungsmethoden sind offen zu legen und durch unabhängige Aufsichtsstellen zu prüfen.

- **Grenzen setzen**: Zweckmäßig wären Verbote für Scorings, beispielsweise durch Vermieter und in Form von Bagatellgrenzen zur Eingrenzung ausufernden Datensammelns.

Datenschutzregeln für geobasierte Dienste auf Smartphones: Smartphone-NutzerInnen sind identifizierbar über UDID/IMEI, Telefonnummer, soziale Netzwerke, Zeit-Weg-Profile, diverse Login-Daten uvm. NutzerInnen benötigen vor allem Schutz vor der Analyse und Ausbeutung ihrer Geodaten (Standort, Bewegungsgeschwindigkeit uä). Ermöglicht wird dies durch die steigende Durchdringung des Marktes mit Smartphones, die mit GPS-Sensoren ausgestattet sind und deren Funktionsumfang mit Apps erweitert werden kann. Die Bewegungsmuster der Geräte können von vielen Akteuren nachverfolgt werden. Sie bieten einen sehr intimen Einblick in das Privatleben der BesitzerInnen. Die Zwecke reichen von Logistik und Verkehrsmanagement über Direktmarketing bis zur Kontrolle der Kinder auf dem Schulweg. Dabei wird in vielen Fällen das Grundrecht auf Privatsphäre und Datenschutz zum Zweck des Profits missachtet.

Viele Apps sind reine Fassaden, die ihren eigentlichen Zweck, nämlich das Datensammeln, verschleiern. Die Verfügbarkeit von Geodaten und die genaue Zuordenbarkeit der einzelnen Geräte zu bestimmten Personen ermöglicht Werbetreibenden eine neue Dimension der Profilerstellung. NutzerInnen sind sich dessen kaum bewusst. Hersteller und Datensammler dürfen nicht davon ausgehen, dass ihre KundInnen technisch versierte Personen sind, nur weil sie im Besitz eines Smartphones sind. Hersteller und Service-Anbieter entledigen sich ihrer Verantwortung. Datenschutzeinrichtungen sind kaum in der Lage, bestehendem Recht zur Durchsetzung zu verhelfen, was auf Grund der nationalen Zuständigkeiten, der unübersehbaren Menge an Apps und der hohen Dynamik in diesem Feld kaum gefordert werden kann.

- **Binnenmarktproblem lösen:** Alle KonsumentInnen in Europa sind gleichermaßen nachteilig betroffen. Geodaten haben eine enorme Binnenmarktrelevanz. Deshalb läge es an der EU-Kommission, europäische Datenschutzstandards gegenüber den großen Hard- und Softwarefirmen durchzusetzen und von Betreibern wie Apple und Google eine Überprüfung ihrer zahlreichen Geschäftspartner zu verlangen.

- **Überwachung mit neuer Dimension**: Die Überwachung fester Orte (bspw mittels Videoüberwachung) wird nun von einer Kontrolle einzelner sich bewegender Menschen mit ihren digitalen Gadgets abgelöst. Es fehlt eine breite gesellschaftliche Diskussion über die Folgen dieses Trends. Soll es in Zukunft bspw als zumutbar gelten, sich selbst einer Überwachung zu unterwerfen, wenn damit bspw günstigere Versicherungsbedingungen einhergehen? Ansätze dazu sind bereits zu erkennen. Einem allzu schnellen Tausch persönlicher Freiheiten gegen ökonomische Vorteile und die Aushöhlung des Solidaritätsprinzips sollte eine klare Absage erteilt werden.

- **Mehr Selbstbestimmungsrechte:** Unternehmen sollten dazu verpflichtet werden, klar darüber zu informieren, welche Daten sie sammeln, und wie sie diese nutzen – bspw durch einen jährlichen Bericht über die über sie gespeicherten Daten an alle NutzerInnen. Die verschiedenen App-Anbieter und Datensammler müssen sicherstellen, dass BesitzerInnen eines mobilen Endgeräts ausreichend über die wichtigsten Elemente der laufenden Datenverarbeitung informiert sind. Dazu zählen bspw der Zweck der Datenverarbeitung, die Dauer, der Umfang und Typ der verwendeten Daten, sowie die Möglichkeit für die Betroffenen, ihre Rechte auf Auskunft, Richtigstellung und Löschung ihrer Daten geltend zu machen.

- **Leichte Erkennbarkeit durch Piktogramme:** Bei der Entwicklung des Betriebssystems ist eine permanent sichtbare Funktion zu integrieren, die darüber informiert, dass Standortdaten verarbeitet werden. Am Markantesten wäre ein sichtbares Zeichen am Display eines Smartphones, das jedes Mal, wenn Geodaten verarbeitet werden, aufscheint. Es wäre ein Beitrag zu mehr öffentlichem Problembewusstsein und würde wieder ein gewisses Maß an Kontrolle an die NutzerInnen zurückgeben.

- **Feiner granulierte Zustimmungen**: Die geforderte informierte Zustimmung im Einzelfall ist schon alleine dadurch nicht gegeben, dass eine Zustimmung, wenn überhaupt, nur ein einziges Mal (nämlich während des Installationsprozesses) pauschal eingeholt wird. Benötigt werden feiner abgestufte Einwilligungen zum Datenzugriff.

- **Missbrauchsschutz:** Die EntwicklerInnen sind in der besten Position, zu kontrollieren, dass sich keine Anwendungen am Smartphone befinden, die heimlich den Aufenthaltsort mobiler Geräte mitverfolgen.

- **Datenschutzgütesiegel:** Wenn NutzerInnen sicher sein könnten, dass Apps nur das tun, was man von ihnen erwartet, wären sie eventuell auch dazu bereit, für dieses Service mehr zu zahlen. Insofern könnten mehr Kontrollen im Vertrieb dazu beitragen, die „schwarzen Schafe“ unter den Apps loszuwerden. Dieses Transparenz- und Vertrauensproblem könnten auch Zertifizierungen beheben, bspw mit dem europäischen Datenschutzgütesiegel „EuroPriSe“.

Mindestharmonisierung für weitere datenschutzsensible Sektoren oder Techniken: Nahezu jede technische Anwendung zieht mehr oder weniger dringliche Fragen und Bedenken hinsichtlich der Vertraulichkeit und der Sicherheit von Daten nach sich, wenn sie zur Sammlung und Verbreitung persönlicher Daten genutzt werden kann. Die abstrakten Regeln für Datenschutz und Datensicherheit müssen in solchen neuralgischen Bereichen auf konkrete Ausübungsregeln und Nutzerrechte heruntergebrochen werden. Dazu zählen verbindliche Regeln:

- **für die Nutzung von Funkfrequenzkennzeichnung**. Mit RFID-Technik können Informationen zwischen einem Funketikett und einem Lesegerät ausgetauscht werden, einer drahtlosen Einrichtung, die diese Informationen über Funkfrequenzen identifizieren kann. RFID-Chips finden sich in vielen Objekten. Damit lassen sich die Herkunft von Lebensmittel und die logistischen Wege von Waren genauso nachvollziehen, wie zB der Aufenthaltsort von PatientInnen.

- **für den Einsatz von Biometrie.** Die Verfahren dienen der automatisierten Erkennung von Personen. Dabei werden individuelle physiologische Merkmale (Fingerabdruck, Gesichtsbild, Muster der Iris) oder verhaltensbedingte (Schreibverhalten, Lippenbewegung, Stimme) dafür herangezogen, eine Person zu identifizieren. Biometrie bietet keine 100%ige Erkennungssicherheit. Dennoch wird sie im Sicherheitsbereich bei der Strafverfolgung, bei Ausweisdokumenten oder auch für Zutrittskontrollen genutzt. Bei der Prüfung der Zugriffsberechtigung zum PC und im bargeldlosen Zahlungsverkehr ist das Verfahren ebenso einsetzbar.

- **für elektronische Zahlungsmittel.** Über Paypal, Paybox & Co hinaus werden künftig noch mehr Zahlungsdienste (zB Google Wallet) elektronische Geldbörsen anbieten. Anbieter, die keine herkömmlichen Banken sind, könnten sich dabei auf das Geschäftsziel stürzen, Kenntnisse der Kaufgewohnheiten ihrer KundInnen zu versilbern.

- **für Connected Cars.** Autos werden zunehmend fahrende Computer, die über Sensoren mit ihrer Umgebung kommunizieren. Vernetzte Fahrzeuge können schon heute eine Vielzahl an Bewegungs-, Zustands-, Verschleiß- und Umgebungsdaten dem Handy des Fahrers, dem zuständigen Autohändler bzw der Vertragswerkstätte melden. Günstig im Notfall und im Falle von Rückholaktionen. Aus Datenschutzsicht aber ein völlig unzureichend geregeltes Gebiet. Elementare Fragen, wie „wem gehören die Daten und wer hat Zugriff darauf“ sind zu regeln.

- **für intelligente Zähler.** Smart Meter sind „intelligente“ Zähler für Strom oder Gas, die den Energieverbrauch und die Nutzungszeit anzeigen, online angebunden und fernauslesbar sind. Auch der Energiebezug ist darüber frei- und abschaltbar. Die österreichischen Netzbetreiber sollen bis Ende 2019 95 % aller ans Netz angeschlossenen Zählpunkte damit ausstatten.

Die Erfassung der Verbrauchsdaten gestattet weitreichende Rückschlüsse auf Lebensgewohnheiten der KundInnen. Aufgrund der Fernabschaltbarkeitsfunktion ist eine Gefährdung der kritischen Infrastruktur und der Versorgungssicherheit der Bevölkerung nicht auszuschließen. Datenschutz und – sicherheit sind ansatzweise geregelt, lassen aber etliche Fragen offen.

- **für öffentliche digitale Anwendungen** wie die elektronischen Patientenakte (ELGA), Online- Abfragen des Pensionskontos uvm. Die Identifikation der Person wird dabei meist mit der elektronischen Bürgerkartenfunktion realisiert. Fragen der Datensparsamkeit in der Verwaltung, der Sorge der Verknüpfung bislang getrennter Datenbestände, Missbrauchsszenarien (im Fall von Patientendaten zB durch private Krankenversicherungen, beim Pensionskonto durch private Finanzdienstleister) und des Selbstbestimmungsrechts der Betroffenen über die Teilnahme an Systemen (Opt In oder Opt Out) stellen sich dabei regelmäßig. Datenschutz und –sicherheit sind üblicherweise geregelt, lassen aber oft auch viele Fragen offen.

Datenschutz und Werbung – vor allem besserer Schutz von Kindern: Digitale Medien spielen im Alltag von Kindern eine selbstverständliche Rolle. Bereits im Vorschulalter gibt es erste Kontakte mit dem Internet. Im Alter zwischen 6 und 10 Jahren steht 59% der Kinder privat ein Internetzugang zur Verfügung. Immer häufiger sind es auch die mobilen Endgeräte (Smartphones, Tablets etc.) der Eltern, mit denen Kinder spielen, Videos ansehen oder im Internet surfen. Dabei kommen Kinder mit verschiedensten Formen von Onlinewerbung und den Methoden kommerzieller Übervorteilung in Berührung. Beworbene Inhalte können sofort konsumiert werden (zB Apps oder In-App-Käufe). Sie kosten im Einzelfall nur wenig. Kosten können sich aber auf diese Art rasch summieren.

Zu den fundamentalen Werbegrundsätzen zählt: Werbung darf das Recht auf Privatsphäre nicht verletzen. Sie muss klar als solche erkennbar sein. Sie darf keinen (in-) direkten Kaufzwang auf Minderjährige ausüben. Diese Prinzipien haben im Internet wenig Gewicht. Es wird mit Mailwerbung gespammt, individuelles Nutzungsverhalten durch Trackingmethoden heimlich nachverfolgt und dabei gewonnene Daten rechtswidrig verwertet. Werbung und redaktionelle Beiträge verschmelzen ununterscheidbar. Und auch die Kleinsten werden mit direkten Kaufappellen auf Webseiten und in Gratis-Apps manipuliert.

- **Facebook:** Nicht-werbliche werden mit werblichen Inhalten im Newsstream vermischt. Deren Erscheinungsform, Rhythmus und auch generelle „Daseinsberechtigung“ (warum bekomme ich diesen Inhalt überhaupt) ist für die NutzerInnen schwer nachvollziehbar. Facebook setzt aber nicht nur auf herkömmliche Werbeanzeigen, sondern nutzt die Interaktionen und sozialen Gefüge seiner NutzerInnen für „soziale“ Werbung. Dabei werden bezahlte Inhalte (gekennzeichnet mit dem Zusatz „Gesponsert“) mit den Online-Aktivitäten und -Interaktionen der eigenen Facebook-Freund/innen verknüpft. Empfiehlt nun der Freund/die Freundin tatsächlich ein Produkt, oder doch nicht? Oft werden nur „Verbindungen“ innerhalb des Netzwerks ausgelesen und die vermeintlich „empfehlenden“ Freunde wissen nichts von ihrer Werbehilfe.

- **Belohnungssysteme in Spielen**: Onlinespiele integrieren das vor allem für Kinder reizvolle Angebot, Kaufwährung als Spielgeld für das Spiel erwerben zu können, indem aktiv Werbung konsumiert wird.

- **Werbung in Apps:** In-App-Werbung ist für Kinder und Jugendliche nur in wenigen Fällen transparent. Während Bannerwerbung gut erkennbar ist, trifft dies auf die meisten Formen der In-Game Werbung nicht zu. Werbung ist oft so gestaltet, dass sie aktionsbehindernd ist. Sie führt immer wieder zu ungeeigneten Inhalten für Kinder. Werbung für andere Apps beinhaltet oft eine direkte Kaufaufforderung. Junge NutzerInnen landen dabei häufig bei Angeboten mit nicht realisierbarem Nutzen (wie zB Gefühls-Scanner oder Lebenserwartungsprognosen).

- **In-App-Käufe:** Sie verfolgen zB das Ziel, die NutzerInnen eines Spieles zum Erwerb von „Kaufwährung" zu bewegen (um damit Premiumangebote zu nutzen). Diese Zusatzleistungen können mit Spielgeld erworben werden, das kostenpflichtig über den App-Shop erworben werden kann. Kinder nehmen oft den kommerziellen Charakter dieser In-App-Käufe nicht wahr. In den App-Beschreibungen wird oft auf In-App-Käufe nicht hingewiesen. Sie sind häufig als unzulässige direkte Kaufaufforderungen an Kinder zu bewerten und nicht selten auch spielbehindernd. Unklar ist, wie wichtig die Nutzung von In-App-Käufen für den Spielverlauf ist. Manche Spiele sind bereits nach kurzer Spieldauer nicht mehr spielbar, ohne einen In-App-Kauf zu tätigen. Sind von Eltern keine entsprechenden Maßnahmen (zB Sperre von In-App-Käufen) gesetzt, können diese zu einer Kostenfalle werden.

- **Likejacking bzw Clickjacking:** Mit dieser missbräuchlichen Taktik werden unbewusste Aktionen von Facebook-NutzerInnen durch Klick auf einen Link oder „Gefällt mir" ausgelöst. Klickt jemand auf den präparierten Beitrag, wird der Inhalt automatisch und ungewollt zB im eigenen FreundInnen-Netzwerk weiterverbreitet und erweckt den Anschein, der Nutzer hätte den Inhalt selbst gepostet. Die gefälschte Empfehlung wird so schneeballartig weiterverbreitet.

Die „analogen" Werberegeln und der Datenschutz in Bezug auf Kundendaten müssen auch in digitalen Medien beachtet werden. Dazu muss die Art ihrer Umsetzung im Internet präzisiert und ihre Durchsetzung drastisch verbessert werden.

Dazu zählt:

- **Werbung und Sponsoring muss transparent gestaltet sein**, sodass ersichtlich ist, wann NutzerInnen es damit zu tun haben und wann nicht.

- **Werbung darf Kinder nicht überrumpeln** und muss ihrem Alter gerecht werden. Die Altersadäquatheit der Inhalte betrifft sowohl die in der Werbung selbst verwendeten Inhalte, als das beworbene Produkt.

- **Werbung darf Kinder nicht unmittelbar auffordern,** bestimmte Produkte zu kaufen oder Kinder dazu zu animieren, zB Eltern zu überreden diese Produkte für sie zu kaufen.

- **Interaktive Werbung muss die Privatsphäre und den Datenschutz achten**, vor allem offenlegen, wie mit personenbezogenen Daten umgegangen wird. Daten dürfen nicht über das für die Diensterbringung zwingend erforderliche Maß hinaus erhoben und verwendet werden.

- **Das Verhalten der UserInnen etwa über den Einsatz von Cookies zu analysieren** - darauf sind viele Anbieter erpicht. Einer automatischen Analyse des Surfverhaltens, um eine Interessenszuordnung zu Werbezwecken zu ermöglichen, muss eine ausdrückliche, freiwillige Zustimmung des Betroffenen vorausgehen.

- **Datenspuren von Minderjährigen dürfen nicht getrackt werden.**

- **Aktionsbehindernde Werbung ist zu verbieten** (zum Beispiel Pop-Up-Werbung, die nicht geschlossen werden kann; eine Deaktivierung führt zum Aufruf einer neuen Seite uvm).
- Keine Werbung bzw Werbelinks für ungeeignete Inhalte in kinderrelevanten digitalen Medien (Tabak, Alkohol, Pornografie, Glücks- und Gewaltspiele etc).

- **Gewinnspiele, die Daten sammeln**, um diese in weiterer Folge für Werbezwecke zu nützen, müssen transparent über diesen Umstand aufklären und dürfen sich nicht an Minderjährige richten.

- **Allgemeine Geschäftsbedingungen und Datenschutzbestimmungen** sollten in einer altersangemessenen Sprache verfasst sein.

- **In den App-Stores ist bei jedem einzelnen App anzuführen,** dass Werbung und In-App-Käufe im Produkt enthalten sind. Weiters ist anzugeben, ob erst mit dem Erwerb des „Freemium"-Produkts (käufliche Erweiterung des Gratisangebotes) der Nutzungszweck vollständig erreicht wird.

- **Werbung darf keine Schadsoftware verbreiten**. Allerdings ist dazu meist eine Aktion der NutzerIn nötig (zB Öffnen einer Datei im Anhang), durch die im Hintergrund unbemerkt Schadsoftware installiert wird. Werbefinanzierte Dienste haben sicherzustellen, dass zumindest von Werbepartnern keine Malware verbreitet wird.

Schutz von Jugendlichen: Viele Minderjährige sind altersbedingt nicht in der Lage, mit Onlineangeboten kompetent umgehen zu können. Die für die analoge Welt entwickelten Jugendschutzziele müssen in Bezug auf digitale Angebote adaptiert und ernsthafter verfolgt werden:

- **Schulische Medienbildung**: Jugendliche (und deren Eltern) sind in immer kürzeren Abständen mit neuartigen Diensten konfrontiert. Frühzeitige Bewusstseinsbildung ist wesentlich. In den Lehrplänen der Pflichtschulen sollte Medienerziehung in zeitgemäßer Form angeboten werden. Zu den inhaltlichen Schwerpunkten zählt neben der sicheren, verantwortungsbewussten Nutzung von Internet und Handys auch die Vermittlung von urheberrechtlichem Basiswissen. Jugendliche laufen bei der privaten Nutzung von Internetunterhaltung Gefahr, Rechte am geistigen Eigentum zu verletzen. Immer öfter erfordert aber auch die Erledigung schulischer Aufgaben die Einbeziehung von geschützten Werken wie e-Learning-Angeboten und Material, das aus dem Internet herunter geladen wird.

- **Geschäftsfähigkeit im digitalen Zeitalter:** Die rechtsgeschäftliche Selbstverpflichtungsfähigkeit ist je nach Altersstufe zivilrechtlich begrenzt. Die darauf gestützte Rechtsprechung hinkt hinter der Marktentwicklung her. Als geringfügige Geschäfte des Alltags, die Kinder selbständig eingehen können, gelten etwa der Kauf von Süßigkeiten, Busfahrkarten uä. Eine rechtliche Befassung mit dem Zugang von Kindern und Jugendlichen zur Vielzahl neuer Angebote, die gegen Bezahlung relativ niedriger Beträge elektronisch bezogen werden können, ist erforderlich. Rechtsunsicherheit führt dazu, dass Eltern im Zweifel von ihren Kindern verursachte Kosten begleichen. Damit verstärken sie den rechtlich nicht haltbaren Eindruck, Kinder und Jugendliche seien gegenwärtig in ungleich größerem Rahmen selbstverpflichtungsfähig als vor Beginn des Internetzeitalters.

Unsicher ist schon, ob und welche der massenhaften Entertainmentangebote in die Kategorie geringfügiger Alltagsgeschäfte fallen. Die Geringfügigkeitsschwelle ist aber beim Mehrfachkonsum von Inhalten auch zu „Micropayment“-Preisen schnell überschritten.

- **Risikolose Alterskontrolle:** Alterskontrollsysteme im Internet dürfen keine Nachteile für Jugendliche nach sich ziehen. Die Anbieter haben die Pflicht, sicherzustellen, dass Kinder und Jugendliche keinen Zugang zu den nach den Jugendschutzbestimmungen nicht altersgerechten Inhalten haben. Außerdem sind die Anbieter bemüht, sich vor Zahlungsausfällen von den Eltern nicht genehmigter Rechtsgeschäfte Minderjähriger zu schützen. Gängigster Weg: das Abfragen des Geburtsjahres oder das Verwenden von AGB-Klauseln, mit deren Akzeptanz Dienstnutzer erklären, sie seien volljährig. Klauseln werden von Jugendlichen selten beachtet und Altersangaben auch unbedarft gefälscht. Bei über 14-Jährigen steht immer wieder der Betrugsverdacht im Raum, wenn sie Dienste unter Missachtung der Altersbeschränkung nutzen, deren Bezahlung sie finanziell überfordert. Es muss sichergestellt werden, dass Alterskontrollen auf eine Weise umgesetzt werden, die datenschutzsensibel sind und junge NutzerInnen nicht kriminalisieren.

- **Präventiver Schutz vor Belästigungen und Mobbing:** Spezifisch am Cyber-Mobbing – also dem systematischen Belästigen oder Bloßstellen im „virtuellen Raum“ – ist: es kann rund um die Uhr erfolgen, erreicht ein großes Publikum und die TäterInnen agieren (scheinbar) anonym. Es ist mehr als ein dummer Streich. Stalking, also die beharrliche Verfolgung einer Person, ist in Österreich strafbar – das gilt auch fürs Internet. Postings in sozialen Netzwerken oder Foren können Ehrenbeleidigungsdelikte darstellen. Das Mediengesetz, das auch für öffentliche Webseiten gilt, sieht Schadenersatz für Opfer von Übler Nachrede, Beschimpfung, Verspottung und Verleumdung vor. Außerdem verbietet es die Verletzung des höchstpersönlichen Lebensbereichs. Die Anleitung von Jugendlichen zu einem kompetenten Nutzungsverhalten digitaler Medien ist daher wichtig. Schulen benötigen mehr Ressourcen, um zeitgemäße Medienerziehung anbieten zu können.

- **Entkriminalisierung von Jugendlichen beim sogenannten „Sexting“.** Unter Jugendlichen ist es zum Teil Trend, erotische Selbstaufnahmen per Smartphone zu versenden. Damit betreten Jugendliche strafrechtlich dünnes Eis. Vom Straftatbestand pornografischer Darstellungen Jugendlicher gibt es zwar Ausnahmen. Es eröffnen sich dabei Auslegungsspielräume, weshalb zugunsten von Jugendlichen mehr Klarheit zu schaffen ist.

10. Geheimdienstaffäre

Die Enthüllungen des ehemaligen US-Geheimdienstmitarbeiters Edward Snowden haben die exzessiven Spähaktivitäten der NSA und verbündeter Dienste ans Tageslicht gebracht. Die NSA überwachte (und überwacht weiterhin) massenhaft E-Mails und Telefonate rund um den Globus. Vor einer derartigen systematischen Missachtung europäischer Grundrechte sind Europas BürgerInnen nicht ansatzweise geschützt. Seit diese Spionageexzesse evident sind, müssten die Zeichen auf Sturm stehen. Der US-amerikanische Whistleblower zeigte schon Anfang Juni 2013 auf, wie die Vereinigten Staaten und das Vereinigte Königreich seit spätestens 2007 in großem Umfang die Telekommunikation und insbesondere das Internet global verdachtsunabhängig überwachen. Als Rechtfertigung dient lediglich der Hinweis, dass damit terroristischen Anschlägen vorgebeugt werde. In vielen Ländern haben Bürgerrechtsorganisationen gegen die massenhafte Überwachung der Bevölkerung protestiert.

Ob Richtfunk, Überland – und Seekabel oder auch Satellit: alle Verkehrswege und Server von Telekomanbietern können angezapft und laufend überwacht werden.

Welche Konsequenzen gibt es? Die systematische Verletzung der Privatsphäre durch (außer) europäische Nachrichtendienste erfordert raschere Konsequenzen. Die rechtlichen Anforderungen an die Datensicherheit in Kommunikationsnetzen müssen deutlich erhöht werden. Der Vorstandschef der deutschen Telekom äußerte sich 2013 gegenüber Medien kritisch über das „leisetretende" Verhalten der Politik in Bezug auf die „NSA-Affäre". „Die Spitzeleien" hätten „das Vertrauen in zwei Grundpfeiler unserer Gesellschaft, die freie Kommunikation und die Privatsphäre, erschüttert." Die Abhörpraktiken von Geheimdiensten seien „demokratiegefährdend", es sei „Sache der Politik und nicht der Telekommunikationswirtschaft, die Einhaltung von Datenschutzstandards einzufordern" und es sei „fahrlässig, dass so wenig geschieht…"

Vordringlich ist daher:

- **Strenge Standards für die Justiz- und Polizeizusammenarbeit und ihre analoge Anwendung auf Geheimdienste:** Dem Grundrechtsschutz im Richtlinienentwurf über den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit ist auf hohem Niveau Rechnung zu tragen. Die Standards für eine grundrechtskonforme Strafrechtsverfolgung sollten analog auch als Messlatte für die Grenzen geheimdienstlicher Ermittlungspraktiken herangezogen werden.

- **Mehr Rechtsschutz:** Sollen Überwachungstechniken durch staatliche Einrichtungen zur Ermittlung von personenbezogener Daten aus Kommunikationsnetzen eingesetzt werden, braucht es mehr Rechtsschutzgarantien für die Betroffenen. Auch den Spähaktivitäten der Privatwirtschaft sind Grenzen zu setzen. Der Einsatz von „Deep Package Inspection" (DPI) zur Überwachung des Inhaltes von Datenpaketen muss äußerst restriktiv geregelt werden. DPI erlaubt ein lückenloses Abhören, Mitschneiden und Verändern der übertragenen Inhalte. Unter anderem wird sie auch von Rechteinhabern, die Urheberrechtsverstöße im Internet verfolgen, benutzt.

- **Keine beliebigen Metadatenanalysen:** Auch wenn Daten auf rechtmäßige Weise ermittelt wurden, ist nicht jede denkbare Verwertung durch Metadatenanalysen grundrechtlich akzeptabel. „Datamining" ist äußerst grundrechtssensibel, erfolgt nicht immer zu (überwiegenden) berechtigten Zwecken und häufig abseits der Wahrnehmung der Betroffenen (Missachtung von Informations- und Zustimmungsrechten). „Big Data"-Analysen bedürfen daher dringend einer präzisen rechtlichen Ausgestaltung. Allein aus der Zusammenschau von Mobilfunkdaten, IP-Adressen, Browserverläufen und E-Mail-Metadaten ergeben sich aussagekräftige Profile zur Überwachung der Bewegungen und Aktivitäten von Personen. Grenzen des zulässigen Einsatzes sind aufzuzeigen, wenn aus großen Datenmengen – durch Filter, statistische Methoden usw. - auf Verhaltensmuster geschlossen wird.

- **Effektive parlamentarische Kontrolle**: Mit Blick auf die europaweite Gefährdung des Kommunikationsgeheimnisses bei Benutzung der europäischen Netzinfrastruktur besteht Bedarf an einer EU-weiten Kooperation bei der Ausübung parlamentarischer Kontrolltätigkeiten. Nachrichtendienste müssen, um ihren Aufgaben gerecht zu werden, bis zu einem gewissen Grad abseits der Wahrnehmung der Öffentlichkeit arbeiten können. Dieses Privileg erhöht allerdings auch das Missbrauchspotential.

In der Regel unterliegen Nachrichtendienste der Kontrolle nationaler Parlamente, die ihrerseits geeignete Formen internationaler Zusammenarbeit benötigen, um ihrer Kontrollaufgabe auch nur annähernd nachkommen zu können.

- **Präzise Telekombetreiberpflichten**: Angesichts des Risikos einer systematischen Verletzung der Vertraulichkeit der Netzkommunikation müssen die Betreiberpflichten präziser formuliert sein. Auslegungsgegenstand ist dabei insbesondere Artikel 4 der EU-Datenschutzrichtlinie für elektronische Kommunikation. Demnach hat „der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit seiner Dienste zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, dass angesichts des bestehenden Risikos angemessen ist“. Um Transparenz für den Verbraucher zu garantieren, gilt überdies: „Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes die Teilnehmer über dieses Risiko und - wenn das Risiko außerhalb des Anwendungsbereichs der vom Dienstanbieter zu treffenden Maßnahmen liegt - über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten“. Dieser Informationspflicht wird in der Praxis nicht immer entsprochen. Die Betreiber brauchen einheitliche Leitlinien, wie sie ihrer Aufklärungspflicht nachkommen und auf welche Abhilfemöglichkeiten sie sinnvollerweise verweisen können.

- **Pflichten für Anbieter von Exchange Servern:** Anbieter von Netzwerkinfrastruktur, die selbst keine Telekomanbieter im Sinne der einschlägigen EU-Richtlinien sind, müssen denselben telekomrechtlichen Datensicherheitspflichten unterworfen werden. Telekommunikationsanbieter unterliegen zwar selbst Anforderungen bezüglich der Datensicherheit ihrer Netzinfrastruktur. Bedienen sie sich dabei der Unterstützung Dritter, werden typischerweise ihre eigenen Sicherheitspflichten dem Dritten im Wege von bloßen Dienstleisterverträgen übertragen. Ob diese Anbieter großer Internetknotenpunkte (wie bspw der Exchange Server in Frankfurt oder Überseekabel, über die der Gesamtverkehr eines oder mehrerer Mitgliedstaaten abgewickelt wird) ihre vertraglichen Datensicherheitspflichten auch einhalten, wird von den Telekomanbietern derzeit in keiner Weise überprüft. Eine Missachtung der rechtlichen Anforderungen, die künftig auch derartigen Dienstleistern aufzuerlegen wäre, sollte Sanktionen nach sich ziehen.

- **Sicherheitsaudit:** Telekomanbieter und Dienstleister, die den überregionalen Gesamtverkehr abwickeln, sollten verpflichtet werden, sich einem verpflichtenden Sicherheitsaudit zu unterwerfen. Die nationalen Telekomregulatoren sehen sich in der Regel nur für Fragen der technischen Netzintegrität verantwortlich und verweisen bezüglich möglicher Verletzungen der Vertraulichkeit des Netzbetriebs auf die nationalen Datenschutzbehörden. Diese sind angesichts ihrer mangelhaften Ausstattung und dem fehlenden branchenspezifischen Knowhow meist nicht in der Lage, Datensicherheitskonzepte und ihre Umsetzung bezüglich der gesamten Telekominfrastruktur eines Landes zu bewerten. Deshalb wäre eine gesetzliche Bestimmung nötig, wonach die genannten Unternehmen in regelmäßigen Abständen eine Datensicherheits-Zertifizierung durch unabhängige Experten den Telekomregulatoren und Datenschutzbehörden nachweisen müssen.

11. Schutz geistigen Eigentums und Datenschutz

Das Urheberrecht galt lange als juristische Materie nur für Spezialisten. Wichtig für Verlage, Kreative und die Filmindustrie. Inzwischen stoßen auch InternetnutzerInnen bei Alltagsaktivitäten auf eine Fülle an Urheberrechtsfragen. Das Urheberrecht ist ein Schutzrecht für RechteinhaberInnen. Es berührt aber auch öffentliche Interessen, etwa in Bezug auf den Zugang zu Werken und Information, freien Werknutzungen, aber auch der Beachtung des Datenschutzes und der Privatsphäre. Geraten diese Interessen mit dem Schutzinteresse der RechteinhaberInnen in Konflikt, muss das Urheberrecht sich um einen Interessensausgleich bemühen. Die Ausgleichsmechanismen, die für analoge Medien entwickelt wurden, passen zum Teil nicht ins digitale Zeitalter. Der nationale Gesetzgeber ist in der Ausgestaltung des Urheberechts vorwiegend an internationale und gemeinschaftsrechtliche Vorgaben gebunden. (Durchsetzbare) NutzerInnenrechte sind darin so gut wie nicht enthalten. Anpassungen des Urheberrechts an das digitale Umfeld zielten auf eine weitere Stärkung der Position der RechteinhaberInnen bzw Verwertungsgesellschaften ab. Einige der Maßnahmen beeinträchtigen die Privatsphäre und Informationsfreiheit.

Konsumentenrechte gegenüber Urheberrechten stärken: Was Nutzer mit erworbenen digitalen Inhalten anfangen können oder nicht, regeln die Anbieter einseitig und zu ihren Gunsten über technische Schranken (Digital Right Management Systeme - DRM) und ihre Lizenzbedingungen. Daraus ergeben sich neuartige Abhängigkeiten: Die Onlineanbieter setzen zum Teil bewusst geschlossene Systeme ein, um Nutzer an sich zu binden. Auch Unvereinbarkeiten zwischen Musikdateiformaten und bestimmten Abspielgeräten behindern Nutzer in der freien Nutzung erworbener Musikstücke. Die Anbieter bieten NutzerInnen meist auch keine Sicherheiten, dass die eingesetzte Technik über Zeit unverändert bleibt. So ist nicht ausgeschlossen, dass Nutzer irgendwann unter Druck geraten, entweder die Entwertung des eigenen Musikarchives in Kauf zu nehmen, Softwareänderungen zuzustimmen bzw neue Endgeräte anzuschaffen. Aus Verbrauchersicht sollte es keinen Unterschied machen, ob ein herkömmliches Buch oder ein e-Book gekauft wird. Häufig kollidieren Konsumentenvertrags- und Urheberrechte miteinander. So schließen Lizenzbedingungen beim Online-Kauf von Musik, Spielen uä unter Berufung auf Urheberrechte oft jegliche Gewährleistungsrechte aus. Insgesamt zeichnet sich ein erhebliches Ungleichgewicht in den Rechtspositionen zwischen den Onlineanbietern und ihren Kunden ab. Die Anbieterseite nützt vertragliche und technische Schranken, um traditionell übliche Nutzungsmöglichkeiten (zB Privatkopien) und Rechtsansprüche (zB Gewährleistung) zu beschneiden. Die Nutzerrechte brauchen Stärkung.

Dazu zählt:

- **ein durchsetzbarer Rechtsanspruch auf Privatkopien**. Dies muss auch gegenüber Anbietern aus Drittländern außerhalb der EU gelten, die ihre Dienste europäischen NutzerInnen anbieten. Mit dem Einsatz von Kopierschutzsystemen und durch vertragliche Regeln können freie Werknutzungsrechte völlig ausgehöhlt werden. Im Urheberrecht sollte daher ein durchsetzbarer Anspruch auf digitale Privatkopien verankert werden.

- **Kopierschutztechniken einschränken**: Nur für den privaten Gebrauch erstellte Kopien dürfen keine sanktionsbewehrte Verletzung von geistigem Eigentum darstellen, selbst wenn sie unter Umgehung von Kopierschutztechniken hergestellt wurden. Technische Umgehungsmöglichkeiten sind meist vorhanden. KonsumentInnen setzen sich dabei dem Risiko aus, eine Urheberrechtsverletzung zu begehen. Die unverhältnismäßige Folge: KonsumentInnen werden abgeschreckt, technische Schranken zu umgehen, um für den privaten Gebrauch übliche Nutzungen zu realisieren.

Das eigentliche Ziel wird dabei verfehlt: für gewerbliche Raubkopierer, die in großem Stil Rechte an Werken missachten, sind die Maßnahmen keine Hürde.

- **Mindestvertragsinhalte**: Die Nutzung beim Abruf digitaler Inhalte liegt anders als beim Warenkauf nicht mehr allein in der Disposition der KonsumentInnen. Auf den ersten Blick ist selten erkennbar, wie umfänglich die Verfügungsrechte zB an einer Datei sind. Welche konkrete Gegenleistung dem eingesetzten Geldbetrag gegenübersteht. Die Nutzungsrechte müssen transparent sein. Mit dem entgeltlichen Erwerb müssen Mindestvertragsinhalte verbunden sein. Erwartet werden genaue Leistungsbeschreibungen statt „buy as it is"-Klauseln, die Gewährleistungsrechte faktisch ausschließen. Auch Kopien für alle gängigen Trägermedien und weitere PCs sollten zu den Nutzungsrechten des/r KäuferIn zählen.

- **Interoperabilität:** Auf EU-Ebene muss verstärkt auf die Hersteller eingewirkt werden, Interoperabilität zu gewährleisten. Aufgrund des komplizierten technischen Zusammenspiels von Dateientyp, Downloadsoftware, Kopierschutzsystemen und Abspielgeräten sind die Systeme zueinander oft - seitens der Anbieter strategisch gewollt - inkompatibel. NutzerInnen können dadurch digitale Inhalte unterschiedlichen Formats nicht problemlos nutzen. Da technische Eigenheiten vom Anbieter auch jederzeit geändert werden können, bleibt es alleiniges Risiko des Nutzers, Inhalte so zu archivieren, dass sie auch noch nach Jahren problemlos verwendet werden können.

- **Keine Doppelzahlungen:** Nutzer laufen Gefahr, für Kopien digitaler Inhalte zweifach zu zahlen: einmal in Form einer Direktzahlung an den Anbieter für den konsumierten Inhalt (wobei die Anbieter für jede Verwendungsart - Zahl der Kopien, Nutzung auf weiteren PCs – eigene Entgelte vorsehen können) und ein weiteres Mal in Form von urheberrechtlichen Pauschalvergütungen an Verwertungsgesellschaften (Abgaben auf digitale Trägermedien und Reprografiegeräte). Die beiden Abgeltungsformen sind aufeinander abzustimmen: die Höhe von Pauschalabgaben müsste in dem Maß sinken, wie Nutzungsrechte technisch oder vertraglich eingeschränkt werden.

- **Nutzungsprofile nur mit ausdrücklicher Zustimmung:** Die EU-Art 29-Datenschutzgruppe betonte wiederholt, dass NutzerInnen die Möglichkeit anonymer Transaktionen im Internet erhalten bleiben muss. Insofern muss rechtlich gewährleistet sein, dass auch DRM die Datenschutzrechte der BenutzerInnen wahrt. DRM-Systeme dienen nicht nur dem Zweck der Zugangskontrolle und der Abrechnung. Die gewonnenen Daten können für Konsumprofile und Übermittlungen an Dritte zu Marketingzwecken genutzt werden. Nutzungsprofile dürfen nur mit ausdrücklicher Zustimmung der NutzerInnen angelegt werden. Die Etikettierung (Wasserzeichen, tags) von aus dem Internet rechtmäßig heruntergeladenen Inhalten darf nicht mit der Identität einer Person verknüpft werden, um bspw die Weiterverwendung des Materials nachzuvollziehen.

- **Verhältnismäßigkeit der Rechtsverfolgung durch die Rechteinhaber:** Die Notwendigkeit eines zeitgemäßen Schutzes der berechtigten Interessen von Rechteinhabern ist unstrittig. Weniger klar ist, wie intensiv dem Grundrechtsschutz der InternetnutzerInnen bei der Durchsetzung geistiger Eigentumsrechte Beachtung geschenkt werden muss. Viele der offenen Rechtsfragen bei der Auslegung der EU-Richtlinie über die Rechtedurchsetzung bei geistigem Eigentum berühren die Grundrechte der InternetnutzerInnen. Die E-MRK und eine Vielzahl an EU-Richtlinien sind für die Klärung dieser Fragen einschlägig: die e-Commerce RL, die RL Urheberrechte in der Informationsgesellschaft, die allgemeine Datenschutz RL, die e-Privacy RL.

Schon allein aufgrund ihres frühen Entstehungszeitpunktes bieten einiger der genannten RL kaum Anhaltspunkte zur Lösung anstehender Rechtsfragen. Entsprechende Bedeutung kommt der Rechtsprechung des EUGH zu. Dieser hat zuletzt in einigen Entscheidungen so manche Klarstellung getroffen (Netzsperren – Portal kino.to; Privatkopievergütung für Downloads aus rechtmäßigen Quellen – ACI Adam; keine allgemeine Überwachungspflicht durch Hostprovider – Netlog; gerechter Ausgleich für Vervielfältigungen – Padawan; Speicherung und Bereitstellung von Verbindungsdaten durch Internetprovider – Promusicae uä). Er tendiert allerdings dazu, komplexe Abwägungsfragen zwischen mehreren betroffenen Grundrechten an die nationalen Gerichte zurückzuverweisen.

Der Gesetzgeber sollte Klarheit schaffen, zB in Bezug auf:

- **die formalen Voraussetzungen**, die erfüllt sein müssen, damit Internetprovider zur Auskunft über Kundendaten verpflichtet sind.

- **die Höchstspeicherdauer** von Internetverkehrsdaten durch Internetprovider für Abrechnungszwecke in Hinblick auf Auskunftsbegehren der Rechteinhaber.

- **die Rechtschutzgarantien**, die Mitgliedstaaten zu verankern haben, damit in der Praxis Datenweitergaben nicht überschießend sind. Mit anderen Worten: wer anhand welcher Kriterien sicherstellt, dass zwischen der Schwere der behaupteten Urheberrechtsverletzung und der Schwere des Grundrechtseingriffes (Datenschutz, Privatsphäre, Informations- und Meinungsfreiheit) ein angemessenes Verhältnis besteht.

- **die Abgrenzung zwischen schwerwiegenden, gewerbsmäßigen Urheberrechts-verletzungen** in Gewinnabsicht und dem gängigen Verhalten von Verbrauchern, urheberrechtlich geschützte Werke zum Privatgebrauch zu nutzen.

- **die Unterscheidung zwischen urheberrechtlich rechtmäßigem und unrechtmäßigem Verhalten** von Internetnutzern: zB (Un-)Zulässigkeit der Umgehung von technischem Kopierschutz abhängig von der „Wirksamkeit“ einer Kopierschutzmaßnahme oder die Nutzung von Streamingdiensten.

- **der genaue Umfang der Maßnahmen**, die Zugangsprovider aufgrund ihrer „Vermittler“-Rolle ergreifen müssen.

- Wie sich **Schadenersatzforderungen** bemessen.

Dabei ist jedenfalls zu berücksichtigen:

- **Richtervorbehalt:** Alle grundrechtssensiblen Rechtsverfolgungsmaßnahmen sind ausnahmslos einem Richtervorbehalt zu unterwerfen. Außergerichtliche Eingriffe in die Nutzerrechte sollten nicht zulässig sein. Internetprovider können nicht selbständig über Datenweitergaben, Filtermaßnahmen bzw Kundensperren entscheiden. Sie können weder das Tatsachenvorbringen des Rechteinhabers abschließend beurteilen, noch den Einzelfall rechtlich bewerten. Laut EUGH ist der Richtervorbehalt im derzeitigen Richtlinienbestand nicht obligatorisch vorgesehen, aber grundrechtlich unter Umständen geboten. Es braucht die Rechtsschutzgarantien eines fair trials – Beachtung der Unschuldsvermutung, ein Ermittlungsverfahren, das beiden Standpunkten Gehör schenkt, Berufungsmöglichkeiten gegen Entscheidungen uvm.

- **Keine generellen Überwachungspflichten** der Internetprovider bzw sonstige Maßnahmen, mit denen in Kauf genommen wird, dass auch in die Rechte von Nutzern, die keine Rechtsverletzung begangen haben, eingegriffen wird. Das bedeutet, dass Internetprovider nicht über den konkreten Anlassfall hinaus standardmäßig in den Kampf gegen Urheberrechtsverletzungen einbezogen werden. Generelle providerseitige Filtermaßnahmen über die gerichtliche Anordnung im Einzelfall hinaus müssen untersagt sein. Mit anderen Worten: keine präventive allgemeine Überwachung des Internetverkehrs, da dies nur unter der Abkehr von elementaren Grundsätzen wie der Unschuldsvermutung, Informationsfreiheit und dem Datenschutz möglich wäre. Verbot des Einsatzes von „Deep Packet"-Inspektionen. Ein derartiges Durchkämmen von Internetdaten mittels Software nach urheberrechtlich geschütztem Material verletzt den Grundsatz der Vertraulichkeit der Kommunikation gegenüber allen Internetnutzern.

- **Keine Kriminalisierung von Verbrauchern**. Das bedeutet, dass strafrechtliche Konsequenzen nur für Urheberrechtsverletzer vorzusehen sind, die gewerbsmäßig in Gewinnabsicht handeln. Gängiges Verbraucherverhalten, für eigene, private Zwecke via Internetstreaming oder digitaler Privatkopien insbesondere Musik-, Video- oder Filmwerke zu konsumieren, ist davon klar abzugrenzen. Für Verbraucher sind auch die zivilrechtlichen Folgen (Kostenersatz für das Einschreiten des gegnerischen Rechtsanwaltes zur Abgabe einer Unterlassungserklärung, Schadenersatz) drakonisch genug. Der unscharfe Begriff eines Urheberrechtsverstoßes „on commercial-scale" schützt Verbraucher, die Werke unberechtigt zum privaten Gebrauch benutzen, nicht ausreichend vor einer strafrechtlichen Verfolgung.

- **Alternativen zum Versuch flächendeckender Rechtsverfolgung** – allen voran akzeptable Geschäftsmodelle. Die Verbraucherorganisation BEUC weist darauf hin, dass die Einnahmenverluste für die Musik- bzw Filmbranche durch Filesharing-Plattformen auch durch noch so rigide Rechtsverfolgung der privaten Nutzer nicht kompensiert würden. Denn es fehlt vielfach schlichtweg an attraktiven, entgeltlich nutzbaren Alternativen. Zu prüfen ist auch, inwieweit die Konzentration der Bemühungen auf eine drakonische Rechtsverfolgung nicht auch für den EU-Raum innovationshemmend wirkt.

- **Es fehlt ein Binnenmarkt für Online-Content**. Die Grundlagen der nationalen Verwertungsgesellschaften – vor allem national erteilte Lizenzen - stehen einer grenzüberschreitenden Nutzung von entgeltlichen Onlinediensten nicht selten entgegen. Es gibt überzeugende Argumente, dass sich die Regulierungsarbeit weniger auf die (in vielen Fällen in globalen Netzwerken aussichtslose) Rechtsdurchsetzung konzentrieren sollte. Vielmehr sollte hinterfragt werden, ob der Urheberrechtsrahmen in dieser Form noch zeitgemäß ist. NutzerInnen finden im digitalen Zeitalter kein ausbalanciertes System zwischen den ausschließlichen Rechten des Urhebers und freien Werknutzungsrechten mehr vor. Es ist hoch an der Zeit, die RL über Urheberrechte in der Informationsgesellschaft aus dem Jahr 2001 verbraucherfreundlich zu überarbeiten.

- **Gewährleistungsregeln für digitale Güter:** Der Anspruch der Rechteinhaber auf einen gerechten Ausgleich für private Vervielfältigung ist unstrittig. Die geübte Praxis bedarf aber einer kritischen Betrachtung. Derzeit werden Verbraucher nicht selten zweimal für ihre Nutzung zur Kasse gebeten: einmal beim Kauf von leeren Datenträgern in Form der Urheberrechtsabgaben und ein weiteres Mal beim Erwerb digitaler Produkte, bei denen der Rechteinhaber allein bestimmt, ob er Kopien überhaupt und wenn ja in welchem Umfang gestattet.

Im ungünstigsten Fall ist der Leistungskern auf ein digitales Konsumangebot beschränkt, über das der Verbraucher mangels einer physischen Kopie auf seiner Festplatte gar nicht selbständig verfügen kann. Spezifische Gewährleistungsregeln für nicht physischen, im Netz abrufbaren digitalen Content wurden vielfach gefordert – Eingang in den EU-Rechtsrahmen fanden sie bislang nicht.

- **Schadenersatzforderungen** können nur der europäischen Tradition folgend auf den konkret nachweisbaren finanziellen Verlust abstellen: Schadenersatzforderungen sollten auf den tatsächlichen konkreten Umsatz- bzw Gewinnentgang abstellen, hierfür einen Ausgleich schaffen, aber dürfen keinesfalls angelehnt ans US-Recht auch abschreckenden Strafcharakter haben.

- **Schutz vor einer „Abmahnindustrie“:** Mit einer Streitwertbegrenzung, Bagatellgrenzen für Sanktionen und Schlichtungsverfahren soll verhindert werden, dass Rechtsanwälte sich auf eine massenhafte Abmahnung privater NutzerInnen spezialisieren und auch unseriöse Akteure auf den Plan rufen, die fingierte Forderungen stellen. Die Dringlichkeit einer Regelung zeigt folgender Fall: für die Nutzung eines geschützten Fotos auf einer nichtkommerziellen Website wurde von einem österreichischen Internetnutzer 2.800 Euro an Lizenzentgelt, Schadenersatz und Anwaltskosten gefordert. Der gleiche Sachverhalt nach deutschem Recht wäre mit rund 750 Euro gedeckelt.

- **Verbraucher- und Datenschützer** sind in viel stärkeren Maß als gegenwärtig in den Regulierungsprozess einzubeziehen.

12. Schutz weiterer Rechte im Internet

Gut koordinierte Netzpolitik befasst sich mit vielen Aspekten der global vernetzten, digitalen Medien. Im Fokus stehen Fragen rund um die Netzwerke, etwa Fragen der Domainregulierung, der technischen Standards, aktuell zB auch Themen wie Netzneutralität oder die Vergabe einmaliger Internetadressen durch die Netzverwaltungsorganisation ICANN. Unzählige Rechtsmaterien berühren die Entwicklungen im Internet. Ob Jugendschutzbestimmungen, Strafrecht, Urheberrecht, das Konsumentenschutzgesetz oder Medienrecht – Netzpolitik erweist sich rasch als denkbar weite Querschnittsmaterie, die auch regierungsseits entsprechend intensiv koordiniert werden muss. Auch der Einfluss digitaler Medien auf die politische Willensbildung, die Netiquette (der respektvolle Umgang im Internet in Zeiten von „Shitstorms“/ Entrüstungsstürmen im Netz) und die Entwicklung von E-Government zählen zu den Themenfeldern, die systematisch zu bearbeiten sind.

Ein Zentrum für netzpolitische Studien. Regierung, Parlament, aber auch die Interessenvertretungen von Verbrauchern und ArbeitnehmerInnen würden von einem Kompetenzzentrum profitieren, das die digitalen Entwicklungen im Detail mitverfolgt und bewertet. Benötigt werden bessere Grundlagen für die rechtspolitische Arbeit in Form von Studien, Marktüberblicken, nutzerbezogenen Praxistests und Handlungskonzepten.

Beteiligung von Stakeholdern: Je nach Interessenshintergrund sehen die Vorstellungen einer Internetregulierung komplett unterschiedlich aus. Die Väter des Internets der siebziger Jahre vor allem aus dem universitären Bereich begründeten ihren historischen Erfolg hauptsächlich mit der Offenheit des Netzes, dem dezentralen Zusammenspiel Einzelner. Entwickler stünden nach Einschätzung des Netzaktivisten Sascha Lobo praktisch ständig vor der Weggabelung zwischen „Zentralismus oder Autarkie, System- oder Nutzerstärkung, Sicherheit oder Freiheit“.

Zeichen dieser Freiheit sind vom Nutzer frei programmierbare Computer: „Aus der Sicht eines kontrollfixierten Sicherheitsfans“ ein hohes Risiko, denn „die Installation von Software ist so leicht, dass dies häufig aus Versehen passiert, weshalb Computer von Viren befallen werden können, Fernseher aber nicht, obwohl sie doch auch irgendwie an einem Netz hängen…Sie bieten genau sechsundsiebzig Funktionen an. Was der Hersteller nicht eingebaut hat, lässt sich auch nicht nachrüsten.“ (Sascha Lobo 2012; Internet Segen oder Fluch). Bei Smartphones sind die programmierbaren Eigenschaften beschränkt. Bei Apple darf neue Software nur dem eigenen App Store entnommen werden. Wenn Apple nicht will, lassen sich andere Programme nicht installieren. Hersteller können über rigide Kontrollen schädliche Inhalte rasch entfernen. Gleichzeitig wird damit die freie Wahl der Verbraucher beschränkt. Die Gerätehersteller könnten auch darüber entscheiden, welche Netzinhalte dargestellt oder ausgefiltert werden. Die offene Netzstruktur muss immer neu abgesichert werden. Hersteller und ihre Techniker sollten nicht allein darüber entscheiden. Es besteht ein öffentliches Interesse an einer institutionalisierten Mitwirkung von zB VertreterInnen von Datenschutz-, Verbraucher-, Wissenschafts- und Wettbewerbsinteressen an wichtigen technischen Weichenstellungen für die Zukunft.

Netzneutralität: Auch das Thema Netzneutralität belegt, dass Laissez Faire keine Handlungsoption ist. Es braucht einen gesetzlichen Rahmen, der einen Zerfall des Netzes in verschiedene Unterklassen abhängig von der Zahlungsfähigkeit der Diensteanbieter und Nutzer verhindert. Gegenwärtig versuchen einige Internetzugangsanbieter ihr Netzwerkmanagement und ihre Geschäftsmodelle europaweit so auszurichten, dass der Grundsatz der Netzneutralität in Frage gestellt wird. Regulatorische Maßnahmen sind nötigt, die die Nutzerinteressen schützen – und zwar in Hinblick auf Transparenz, Achtung der Grundrechte (Informationsfreiheit, Datenschutz, Schutz der Privatsphäre), Angebotsvielfalt und Wahlfreiheit, Qualität der Dienste und Bekämpfung unfairen Wettbewerbs und der Förderung innovativer Dienste. Verbraucher müssen darauf vertrauen können, dass der Zugang zum Internet uneingeschränkt offen bleibt. Mit anderen Worten: der gesamte Netzcontent muss ohne Bevorzugung oder Benachteiligung einzelner Kunden oder einzelner Dienste vom Internetprovider dargestellt und transportiert werden. Steuernde Eingriffe in den Datenstrom sind nur aus zwingend technischen Gründen - für Zwecke der Datensicherheit und Netzintegrität bei Netzüberlastung - zulässig. KonsumentInnen sind über steuernde Eingriffsmöglichkeiten schon bei Vertragsabschluss aufzuklären. Eine Unterscheidung in „vollständige“ Internetzugänge und „zweitklassige“ Zugänge zu günstigeren Preisen, die aber vielfältigen Einschränkungen unterliegen (Geschwindigkeitsdrosselung oder Sperre bestimmter Websites oder Dienste) überfordert KonsumentInnen. Es erschwert die Vergleichbarkeit von Angeboten und ist strikt abzulehnen. Erklärtes EU-Ziel sollte sein, den Infrastrukturausbau voranzutreiben. Damit stünde auch längerfristig allen KonsumentInnen genug Bandbreite zur Nutzung eines uneingeschränkten offenen Internetzugangs zur Verfügung.

- **Ein EU-Verordnungsvorschlag über den Binnenmarkt für Kommunikationsdienste** untersagt zwar „innerhalb vertraglich vereinbarter Datenvolumina oder –geschwindigkeiten für Internetzugangsdienste Blockierungen, Verlangsamung, Diskriminierungen bestimmter Inhalte“. Durch die gleichzeitige Akzeptanz von Vereinbarungen über die „Erbringung von Spezialdiensten mit einer höheren Dienstqualität“ wird das Verbot aber weitgehend entwertet. Internetprovider könnten exklusive Verträge für die Übertragung in besserer Qualität mit bestimmten Inhaltsanbietern schließen. Verlangt wird nur, dass die „allgemeine Qualität des Internetzugangs“ durch solche Exklusivverträge nicht beeinträchtigt wird. Für den Verbraucher würde es noch schwerer, den Marktüberblick zu bewahren und passende Kaufentscheidungen zu treffen. Bei günstigen Breitbandzugängen könnte dies bedeuten: E-Mail und Websurfen sind unproblematisch, Videoschauen in hoher Auflösung geht nur gegen Aufpreis.

- **Auch die Privatsphäre steht dabei auf der Kippe**. So experimentieren Betreiber mit Modellen, bei denen das Surfverhalten des Kunden überwacht wird. Der Zugang zu datenintensiven Streamingdiensten wird nach Verbrauch einer bestimmten Datenmenge nur mehr geschwindigkeitsgedrosselt angeboten.

Das Prinzip der Netzneutralität ist daher zum Schutz der InternetnutzerInnen ausreichend abzusichern. Konzerne wie Google, Apple & Co können sich andernfalls für ihre Angebote Schnellstraßen in Form exklusiver Qualität teuer erkaufen. Kleine Anbieter bleiben dabei auf der Strecke. Für die Vielfalt und Innovationen im Internet sind sie jedoch besonders wichtig.

Marktkonzentration: Es gibt eine enorme Vielfalt im elektronischen Handel. Die kleinste Frühstückspension im entlegensten Tal profitiert von der unbegrenzten Reichweite ihrer Webpräsenz. Neben diesem überaus bunten Angebotsspektrum gibt es eine immense Marktkonzentration. Globale Konzerne wie bspw Google, Amazon und Facebook haben eine Monopolstärke entwickelt, der auch nationale Regierungen und EU-Einrichtungen nicht gewachsen sind. Der Mapping-Dienst Google-Street-View sollte bspw strenge Verhaltensstandards durch die Datenschutzkommission verordnet bekommen. Google reagierte – zum Nachteil jener, die in dem Dienst einen Mehrwert sahen – mit einem kompletten Rückzug des Dienstes vom – aus Betreibersicht wenig relevanten - österreichischen Markt. Die enorme Marktkonzentration gefährdet jedenfalls den Wettbewerb oder schließt ihn sogar aus. Ziel muss es sein, auf Europa-Ebene mehr Wettbewerb im Internet durchzusetzen. Innovationsfördernd wäre auch die breite Unterstützung von Open Source- bzw-freier Software, bei der der Quelltext offengelegt und auch Dritten eine Weiterentwicklung der Programme ermöglicht wird.

Open Data: Open Data steht für die Idee, (meist öffentliche) Daten allgemein verfügbar und nutzbar zu machen. Potentiale hinter den Daten, die Behörden und Ministerien, Parlamente, Gerichte und andere Teile der öffentlichen Verwaltung produzieren, sollen gehoben werden. Was man mit den Umwelt- und Wetterdaten, Geodaten, Verkehrsdaten, Haushaltsdaten, den Statistiken, Publikationen, Protokollen, Gesetzen, Urteilen und Verordnungen alles machen kann, beflügelt unternehmerische Geschäftsideen. Auch die Wissenschaft, Behörden untereinander, Bürgerinitiativen und Einzelpersonen können von einem freien Zugang zu derartigen Informationen und ihrer Weiterverarbeitung profitieren. Neben diesen positiven Aspekten gibt es aber auch nicht wenige – vor allem auch datenschutzrechtliche - Bedenken an einer uferlosen Verwertbarkeit öffentlicher Daten, die unter Umständen nicht ausreichend anonymisiert sind. Auch Fragen der Haftung, des Urheberrechtes usw. bedürfen einer Klärung.

Partizipationsverfahren bei Themen mit großen gesellschaftlichen Auswirkungen: Ob private Videoüberwachung mit kostengünstigen Videokameras aus dem Baumarkt, elektronische Patientenakte oder digitale Stromzähler für alle Haushalte. Derartige Projekte berühren praktisch jeden. Vor und Nachteile dieser Entwicklungen werden kontroversiell diskutiert. Komfort- und Sicherheitswünsche stehen Überwachungs- und Missbrauchsszenarien gegenüber. Regulatorische Entscheidungen, Techniken voranzutreiben, für zulässig zu erachten oder sogar verpflichtend vorzuschreiben müssen von einer breiten Zustimmung der Bevölkerung getragen sein. Information und eine Beteiligung der Bevölkerung an der Diskussion muss breiter als bisher organisiert werden. Es sollte öfter auf Partizipationsmodelle zurückgegriffen werden, über die Betroffene informationell gut eingebunden sind, Sorgen und Ängste Beachtung finden und unerwünschte Folgen oder auch Alternativen gründlich erforscht werden.

13. Maßnahmen gegen Internetkriminalität

Parallel zum Boom des Online-Shoppings, von Sozialen Netzwerken & Co. steigt auch die Häufigkeit von Betrugsfällen. Das Innenressort registrierte 2013 11.200 angezeigte „Cybercrime“-Fälle. Ob Fake-Shops, Immobilien- bzw Treuhand-Betrug über Kleinanzeigen-Plattformen, Phishing-Mails, Markenfälscher, Identitätsdiebstahl, Hacking oder geplünderte Konten: Die Internetkriminalität in Österreich steigt. Auch klassische Straftaten wie Täuschung, Erpressung, Geldwäsche oder Beleidigung können mit Hilfe des Internets vergleichsweise leicht, grenzüberschreitend und oft auch anonym begangen werden. Jede dritte Beschwerde beim Internet Ombudsmann betrifft eine der vielen Formen von Abzocke und Cyberkriminalität im Netz und auch das Bundeskriminalamt berichtet jährlich über mehrere Tausend Anzeigen zu Internet-Betrug. Die Abhängigkeit von der Funktionsfähigkeit des Internets ist derart gestiegen, dass eine intensive Auseinandersetzung mit Aspekten wie Datensicherheit im Internet, Schäden die Hackingangriffe, die Verbreitung von Malware, die gezielte Überlastung von Servern, die Entwendung digitaler Identitäten oder die Manipulation von Daten auch bei privaten Internetnutzern anrichten können, nötig ist.

Strafrechtsreform: Die Grenzen zwischen zivilrechtlich bekämpfbarer Irreführung der Verbraucher und strafrechtsrelevantem Betrug verschwimmen in der Praxis oft. Vor diesem Hintergrund ist eine zeitgemäße Präzisierung des Betrugstatbestandes für das Onlineumfeld nötig, die Möglichkeit der Gewinnabschöpfung in Verbandsverfahren wegen Verstoßes gegen das UWG und eine Verbesserung der Strukturen für die grenzüberschreitende Zusammenarbeit, um das enorme Vollzugsdefizit (mehrheitliche Einstellung der Verfahren, selbst wenn aufgrund der hohen Betroffenenzahl die Streuschäden in Summe hoch sind) zu verringern. Die Einrichtung von Schwerpunkt-Staatsanwaltschaften rund um das Thema Internetkriminalität wäre zweckmäßig.

Außergerichtliche Lösungen erleichtern: Beschwerden über Fake-Accounts häufen sich: Jemand erstellt unter Verwendung eines fremden Namens ein Profil auf Facebook und verbreitet darüber „peinliche“ Inhalte, darunter auch Fotos. Jemand beteiligt sich an einem Video-Chat und wird später von seinem Gegenüber erpresst: bei Verweigerung der Zahlung würde das Video im Internet veröffentlicht. Eine besorgte Schuldirektorin sucht nach Lösungen: SchülerInnen würden auf der beliebten Social Media Anwendung ask.fm bloßgestellt und private Nachrichten und Adressdaten veröffentlicht. Die außergerichtliche Abwicklung von derartigen Löschungsbegehren muss für die Betroffenen vereinfacht werden. Es braucht ein internationales Kontaktnetz über die Betroffene rasche Unterstützung bei der Durchsetzung konkreter Löschungsanliegen wegen Identitätsdiebstahls und ihre Person bloßstellender Beiträge erhalten können.

Ressortübergreifende Schwerpunktaktionen: Die zuständigen Ressorts (BKA, Verbraucher-, Bildungs-, Justiz- und Innenministerium usw.) könnten mit Schwerpunktaktionen rund um das Thema „Digitale Welt“ zur Bewusstseinsbildung der Bevölkerung in Bezug auf das richtige Verhalten im Internet beitragen. Vollzugsdefizite in Bezug auf Rechtsverletzungen im Bereich des Datenschutzes, strafrechtsrelevanter Online-Geschäftspraktiken sollten in einer ressortübergreifenden Arbeitsgruppe analysiert und schließlich verringert werden. Anstelle von sich teilweise inhaltlich überschneidenden Einzelaktivitäten der einzelnen angesprochenen Ressorts wird auf ein koordiniertes Zusammenwirken geachtet, um die knappen Ressourcen bestmöglich einzusetzen.

Basisfinanzierung für die Betrugspräventionsarbeit:

- Die **„Watchlist Internet“** (www.watchlist-internet.at) widmet sich der Betrugsprävention durch verbesserte Aufklärung der InternetnutzerInnen. Die „Watchlist“ ist eine u.a. von BMASK und AK geförderte Informationsplattform, über die KonsumentInnen tagesaktuelle Warnungen und Tipps im Umgang mit Internet-Betrug und betrugsähnlichen Online-Fallen erhalten. Über ein Meldeformular können User selbst Betrugsfälle oder Online-Fallen melden und so die Aufklärungsarbeit der „Watchlist Internet“ aktiv unterstützen.

- **Internetombudsmann:** „Wie initiiere ich erfolgreich eine Löschung von Interneteinträgen zu meiner Person.“ „Ein Rechteinhaber verlangt 1000 Euro für die Verletzung seiner Rechte wegen eines Bildes auf meiner Website“. „Muss ich nach dem Hackingangriff bei Ebay mein Passwort ändern.“ Fragen in Bezug auf Datenschutz, Persönlichkeitsrecht, Medien- und Internetrecht nehmen beim Verein Internetombudsmann erheblich zu.

- **Saferinternet.at** unterstützt vorrangig Kinder, Jugendliche, Eltern und Lehrende beim sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien. Die Initiative wurde im Auftrag der Europäischen Kommission im Rahmen des Safer Internet Programms umgesetzt. Da EU-seits die Verlängerung des Programms immer wieder zur Disposition steht, sollte auf eine langfristige Finanzierung seitens der EU-Kommission gedrängt werden oder eine nationale Förderung sichergestellt sein. Neben Beratung, Broschüren und Onlineinformation vermittelt die Initiative auch viele hundert Male im Jahr ReferentInnen rund um das Thema „Sichere Internet- und Handynutzung“ für Workshops, Vorträge, Schulprojekte und Fortbildungen für SchülerInnen, Eltern, Lehrende und SozialarbeiterInnen in ganz Österreich.

Die langfristige Finanzierung dieser Initiativen sollte aus öffentlichen Mitteln sichergestellt werden.

Medienkompetenz quer durch alle Bevölkerungskreise und in jedem Alter fördern: Bloggen, twittern, chatten, mailen, Podcasts hören und selbst produzieren, Webradio und Soziale Netzwerke – das Internet holt neue Welten in die Zimmer von Jugendlichen. Medienkompetenz ist dabei ein wichtiges Stichwort. Souveräner Umgang mit Technik, Datenschutz und Datensicherheit, aber auch Recherchekompetenzen im Internet müssen geübt werden. Auch betriebliche Datenschutzbeauftragte können Informationsdrehscheiben sein, die Wissen an MitarbeiterInnen weitergeben und kritische Diskussionen über risikobehaftete Technologien anstoßen. Das Ziel wäre: Mit einem breiten Einsatz von gut ausgebildeten betrieblichen Datenschutzbeauftragten stünden auch künftige Meinungsbildner zur Verfügung. Sie könnten über ihre betrieblichen Aufgaben hinaus ihr Wissen und eine risikokritische Sicht über technologische Entwicklungen in ihr Umfeld weitertragen.