17. August 2018

Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit

Zusammenfassung

Auftrag

In Umsetzung der Motion Rechsteiner (13.3841) setzte das Eidgenössische Finanzdepartement am 27. August 2015 eine auf drei Jahre befristete Expertengruppe „Zukunft der Datenbearbeitung und Datensicherheit“ ein. Diese erhielt den Auftrag, folgende Fragen aufzuarbeiten:

1. Wie sind die technologischen und politischen Entwicklungen auf dem Gebiet der Datenbearbeitung zu beurteilen?

2. Was bedeuten diese Entwicklungen für die schweizerische Wirtschaft, die Gesellschaft und den Staat?

3. Wie ist der gegenwärtige Rechtsrahmen mit Blick auf diese Entwicklung zu beurteilen?

4. Welche Empfehlungen ergeben sich daraus für die Schweiz? Auf nationaler Ebene? Mit Blick auf mögliche Initiativen auf internationaler Ebene?

Neben einer Erörterung der technologischen Entwicklungen beantwortet die Expertengruppe die Motionsfragen vor dem Hintergrund der umfassenden digitalen Transformation und unter Berücksichtigung ihrer gesamtgesellschaftlichen Dimension. Im Zentrum stehen dabei sechs Bereiche bzw. Analysefelder: Informationssicherheit, das Verhältnis Unternehmen zu Kunden (Business to Consumer; B2C), der Unternehmen untereinander (Business to Business, B2B), des Staates zu den Bürgern/Unternehmen (Government to Citizen/Business; G2Ci/B), digitale Aufklärung der Bevölkerung, Kompetenzaufbau und Mitgestaltung der Nutzer sowie digitale Transformation und Ethik.

Herausforderungen und neue Möglichkeiten

Die digitale Transformation erfasst alle Wirtschafts- und Lebensbereiche. Sie öffnet viele neue Möglichkeiten, führt aber auch zu einer zunehmenden Abhängigkeit der Gesellschaft von verstärkt autonom operierenden Systemen: In allen Lebenslagen wird das Smartphone mitgeführt, welches eine direkte Kommunikation ermöglicht, den Zugang zu Informationen verschafft, neue Anwendungen eröffnet aber auch über das Internet grosse Datenmengen austauscht und eine Vielzahl von Informationen über die Nutzer und von Diensten vermittelt. Angesichts der wachsenden Abhängigkeit unserer Zivilisation von den digitalen Technologien drohen menschliche Kontroll-, Eingriffs- und Entscheidungsmöglichkeiten verdrängt zu werden. Menge, Geschwindigkeit und Detaillierungsgrad von Informationen werden weiter zunehmen. Das Gleiche gilt für die Verfügbarkeit benutzerfreundlicher und für breite Kreise erschwinglicher Hard- und Software. Vernetzbare, mit Sensoren ausgestattete Geräte, die Daten übermitteln, sind allgegenwärtig. Das „Internet of Things“ entwickelt sich zum „Internet of Everything“. Künstliche Intelligenzen quantifizieren, analysieren und bewerten auf der Grundlage selbstlernender Algorithmen unermessliche Mengen angefallener Daten. Zudem steht der Einsatz funktionsfähiger Quantencomputer, die heutige Verschlüsselungsinfrastrukturen wirkungslos machen könnten, bevor.

Digitale Verhaltensüberwachung im öffentlichen Raum oder auf sozialen Netzwerken sowie andere, die Menschen in ihrer selbstbestimmten Lebensgestaltung einschränkende Datenbearbeitungen wie „Big Nudging“ oder „prädiktive Modellierung“ bergen Potenzial für gesellschaftliche Fehlentwicklungen. Die Ethik soll die Grundlagen dafür bieten, diese zu erkennen und aktiv an gesellschaftlich wünschbaren Innovationen mitzuarbeiten.

Ungeachtet der Dynamik der Digitalisierung spricht sich die Expertengruppe gegen einen regulatorischen Aktionismus des Staates aus, zumal die Ordnungsstrukturen wie das Recht und weitere Verhaltensnormen aus der analogen Welt generell auch für die digitalen Herausforderungen ein erhebliches Lösungspotenzial aufweisen. Umso entschlossener sollten aber erkannte Lücken geschlossen und dann Lösungen dynamisch weiterentwickelt werden, wenn traditionelle Lösungen an ihre Grenzen stossen.

Informationssicherheit

Mit der zunehmenden Vernetzung und Komplexität der Systeme steigen die Anzahl unbekannter Schwachstellen im Netz und das damit einhergehende Schadenspotenzial weiter an. Die Erwartungen an einen unterbruchsfreien Betrieb der digitalen Infrastrukturen sind höher als die Betreiber garantieren können.

Digitale Transformation kann nur nachhaltig sein, wenn sie auf Vertrauen in eine technologisch sichere Datenbearbeitung beruht. Die zentralen Erfolgsfaktoren liegen einerseits in einer Verstärkung der Ausbildungsangebote und -inhalte in den Bereichen Informatik und Informationssicherheit, andererseits ist die Schweiz gefordert, zukunftssichere kryptografisch abgesicherte Kommunikationsinfrastrukturen zu schaffen. Deshalb soll der Bund mit dem Aufbau eines nationalen Netzwerks zur Förderung der Forschung im Bereich der Informationssicherheit und des Wissenstransfers zwischen Forschung und Wirtschaft beitragen. Auch soll er, in Abstimmung mit der Entwicklung im Ausland, prüfen, ob und in welchen Bereichen Standards und Zertifizierungen bei Software und cyber-physischen Geräten zu einer Voraussetzung für den Marktzugang von IKT-Komponenten erklärt werden müssen.

Business to Consumer (B2C)

Die Digitalisierung hat zu einer Vielfalt neuer kostengünstiger Angebote geführt. Mittels Tracking und Big Data Analysen erstellen die Anbieter Persönlichkeitsprofile, die zwar einen hohen Komfort und Service ermöglichen, gleichzeitig aber auch zu wirtschaftlicher Übervorteilung sowie schweren Eingriffen in die Privatsphäre und informationelle Selbstbestimmung der Netznutzer führen können. Mit Blick auf einen freiheitsverträglichen und wirtschaftlich fairen Interessenausgleich zwischen Unternehmen und den Abnehmern von Gütern/Dienstleistungen sehen sich der Daten- und der Konsumentenschutz in der digitalen Realität mit einer gesteigerten Erwartungshaltung der Netznutzer nach Aufklärung und Schutz konfrontiert.

In ihren Anstrengungen sicherzustellen, dass Personendaten nicht mit der technisch machbaren, sondern rechtlich zulässigen Intensität unter Einsatz von datenschutzfreundlichen Technologien bearbeitet werden, stossen die mit veralteten Rechtsgrundlagen, beschränkten Befugnissen und unzureichenden Mitteln ausgestatteten Datenschutzaufsichtsbehörden zunehmend an Grenzen. Der Eidgenössische Datenschutz-

und Öffentlichkeitsbeauftragte (EDÖB) und die kantonalen Datenschutzbehörden sollten deshalb baldmöglichst Befugnisse und Mittel erhalten, die es ihnen ermöglichen, ihre Aufgaben in der digitalen Realität mit der nötigen Wirkung und Kontrolldichte wahrzunehmen.

Mit Ausnahme einzelner gewerblicher Regulierungen sowie Konzessionierungsauflagen auf kantonaler Ebene gibt es bezüglich Konsumentenschutz keine Qualitätsauflagen. Ein entsprechender Qualitätslevel soll durch den Wettbewerb sichergestellt werden. Wesentliche Bestandteile des schweizerischen Konsumentenschutzes sind die Preistransparenz und der Schutz vor Täuschung und Vermögensdelinquenz. Die Expertengruppe sieht zurzeit keine Notwendigkeit für einen weiter gehenden Paradigmenwechsel. Der Bund ist jedoch v.a. im B2C-Bereich (und sachgleich im B2B-Kontext) gefordert, in Zusammenarbeit mit der Wirtschaft geeignete Instrumente einzusetzen, um einen angemessenen Konsumentenschutz zu gewährleisten. Zu prüfen sind im Weiteren sektorspezifische Regulierungen zur Verhinderung von Preisdiskriminierung, ein angemessenes Online-Widerrufsrecht, Anpassungen im Vertragsrecht mit Bezug auf digitale Verträge und Inhalte sowie die Einrichtung von Online-Beschwerde- und Streitschlichtungsmechanismen (Online Dispute Resolution, ODR).

Business to Business (B2B)

Die digitale Transformation führt im Bereich B2B zu einer stärker ausgeprägten internationalen Vernetzung und zu einem tiefgreifenden Strukturwandel. Ausdruck davon sind neue Geschäftsmodelle, die unter dem Stichwort „Sharing Economy“ zusammengefasst werden können. Die Regelung und Aufrechterhaltung des Wettbewerbs spielt dabei eine wichtige Rolle. Mit Blick auf die Bearbeitung von riesigen Datenmengen durch private Unternehmen ist der Bund gefordert zu prüfen, ob Anpassungen im Kartellrecht, wie z.B. neue Aufgreifkriterien bei der Kontrolle von Firmenzusammenschlüssen oder eine Regelung zu „Absprachen“ durch Algorithmen, angebracht sind.

Weitere wichtige Herausforderungen für den B2B-Bereich (aber auch für B2C-Rechtsverhältnisse) ergeben sich mit Bezug auf den Datenzugang und das Dateneigentum:

Die Rechtslage in der EU legt es nahe, das datenschutzrechtliche Auskunftsrecht um das Element der Datenportabilität zu ergänzen sowie die Portabilität von Sachdaten und die Ausgestaltung eines Zwangslizenzen-Systems für den Zugang zu Sachdaten zu prüfen.

Die heute bestehenden Lücken mit Bezug auf die Rechte der Betroffenen beim Dateneigentum sind sinnvollerweise durch Anpassungen in den entsprechenden Spezialgesetzen zu schliessen.

Die vor wenigen Jahren entwickelte und immer wichtiger werdende Blockchain-Technologie, die als Grundlage z.B. für Kryptowährungen und Smart Contracts dient, dürfte v.a. für den B2B-Bereich viele Effizienzvorteile und die Grundlage für neue digitale Geschäftsmodelle bieten. Gewisse Risiken sind aber nicht zu übersehen, insbesondere mit Blick auf die Sicherheit und den Datenschutz. Sollte die Blockchain-Technologie etwa für die Registerführung oder staatliche Verfahren (Wahlen) eingesetzt werden, könnte sich ebenfalls ein Handlungsbedarf ergeben. Der Bundesrat sollte deshalb die ausländischen Regulierungsbestrebungen im Auge behalten und ggf. selber legislatorisch tätig werden, wenn sich dies als notwendig erweist.

Government to Citizen/Business (G2Ci/B)

Da der Cyberraum als erweiterter öffentlicher und privater Raum wahrgenommen wird, kommen dem Staat diesbezüglich die gleichen Schutzaufgaben wie in der analogen Welt zu. Er ist auch hier gefordert, der Gesellschaft einen sicheren und leistungsfähigen Datenzugang im Sinne einer Grundversorgung zu ermöglichen.

Bund und Kantone sollen deshalb in enger Zusammenarbeit mit den Fachverbänden verbindliche IKT-Sicherheitsstandards erarbeiten und Betreiber kritischer Infrastrukturen zu deren Anwendung verpflichten. Zu Fragen der Standardisierung ist ein Kompetenzzentrum bzw. eine entsprechende Anlaufstelle nötig.

Den sich stellenden Herausforderungen sollte zudem mit weiteren Programmen zur Verbesserung der Informationssicherheit in der Wirtschaft, einer Meldepflicht für Cybervorfälle für die Betreiber kritischer Infrastrukturen sowie dem Ausbau von MELANI zu einem landesweiten Zentrum zur Prävention und Bewältigung von Cybervorfällen begegnet werden.

Ein Ländervergleich zeigt, dass auch in der Schweiz Handlungsbedarf besteht. In Zusammenarbeit mit Verbänden und Wirtschaft sind Massnahmen an die Hand zu nehmen, um die Wirtschaft zu schützen und zu unterstützen. Dies erfordert einen sicherheitspolitischen Diskurs über den Aufbau notwendiger Mittel und die Kooperation mit anderen Staaten.

Seit über zehn Jahren verfolgen Bund, Kantone und Gemeinden eine aktive E-Government Strategie. Die Open Government Data (OGD)-Strategie hat zum Ziel, Rahmenbedingungen zu schaffen, damit die Verwaltung die erhobenen Daten der Gesellschaft zur Wiederverwertung zur Verfügung stellen kann. Für die Umsetzung dieser Strategie fehlen nach wie vor rechtliche Grundlagen, eine Standardisierung bei der Datenaufbereitung sowie ausreichende Ressourcen. Die laufenden E-Government Projekte, wie etwa die Schaffung eines Rechtsrahmens für ein staatlich anerkanntes E-ID-System oder das Transaktionsportal für die Wirtschaft, sollten beschleunigt, flächendeckend und zusammen mit den Basisinfrastrukturen weitergeführt und -entwickelt werden.

Die digitale Transformation durchdringt zusehends auch das historisch gewachsene Werte- und Normensystem unserer Demokratie. Bund und Kantone sind deshalb aufgefordert, im Bereich der Behördentätigkeiten Rahmenbedingungen zu schaffen, die eine möglichst bürgerfreundliche sowie gut vernetzte Datenbearbeitung unter Wahrung der Datenschutzanliegen ermöglichen. Sie haben aber gleichzeitig auch sicherzustellen, dass die Bevölkerungsgruppe der „Offliner“ durch die Digitalisierung nicht gesellschaftlich ausgegrenzt wird.

Eine grosse Chance ergibt sich im Bereich der Partizipation. Dabei sollten insbesondere innovative Ansätze zur partizipativen Demokratie mit Pilotprojekten gefördert werden. Hingegen soll E-Voting nur ausgedehnt werden, wenn aufgezeigt werden kann, dass es nicht mit grösseren Risiken verbunden ist als die bestehenden Formen der demokratischen Mitwirkung bei Wahlen und Abstimmungen. Insbesondere müssen Wahl- und Abstimmungsergebnisse überprüfbar bleiben.

Digitale Aufklärung der Bevölkerung, Kompetenzaufbau und Mitgestaltung der Nutzer

Es ist Aufgabe der Bildung und Weiterbildung auf allen Ebenen, die Bevölkerung aller Altersstufen auf die digitale Herausforderung vorzubereiten, d.h. sie muss mit Fähigkeiten und Kompetenzen ausgestattet werden, um die Chancen der Digitalisierung verantwortungsvoll nutzen und den Herausforderungen adäquat begegnen zu können. Dazu gehören Grundkenntnisse über Informationsverarbeitung und -nutzung sowie die Fähigkeit, relevante Informationen zu finden und kritisch zu bewerten.

Um dies zu erreichen, sind auf allen Ausbildungsstufen die notwendigen Grundfertigkeiten und Kompetenzen für den Umgang und die Gestaltung mit digitalen Technologien und der Transformation zu entwickeln. Gleichzeitig ist auch die Weiterbildung für Berufsleute in allen Bereichen zu erleichtern.

Digitale Transformation und Ethik

Ein besonderes Gewicht kommt bei der digitalen Transformation der Ethik zu. Die momentan stattfindende Entwicklung der Datenbearbeitung verändert die Gesellschaft tiefgreifend und hat bedeutende Auswirkungen auf zentrale Werte und Grundsätze wie Menschenwürde und Privatsphäre, Gleichheit und Diskriminierungsverbot, Autonomie und Selbstbestimmung sowie Transparenz, Solidarität und Sicherheit.

Es ist die Aufgabe der Ethik, vor möglichen Fehlentwicklungen zu warnen und übertriebene Hoffnungen oder Ängste kritisch zu begleiten. Gleichzeitig soll sie aber auch über innovative Lösungen aufklären. Dies verlangt ein besonderes Bewusstsein, inwieweit Grundwerte beeinträchtigt oder gestärkt werden können.

Bund und Kantone müssen deshalb ihre diesbezügliche Verantwortung wahrnehmen und sich dafür einsetzen, dass der Schutz von Grundwerten, Menschenrechten und Menschenwürde auch im digitalen Zeitalter gesichert ist und das Bewusstsein für die informationelle Selbstbestimmung gefördert wird. Die Ethik soll deshalb zu einem festen Bestandteil der Aus- und Weiterbildung werden.

Abschliessend hält die Expertengruppe fest, dass die Entwicklungen im Bereich der Datenbearbeitung und -sicherheit rasch voranschreiten und deshalb die Frage des weiteren Handlungs- und Anpassungsbedarfs für die Schweiz einer andauernden Analyse und Beurteilung bedarf.

Empfehlungen

Die Reihenfolge der Empfehlungen widerspiegelt keine Priorisierung, sondern die Reihenfolge der Themen im Bericht.

Analysefeld Informationssicherheit

Ausbildung im Bereich Informationssicherheit

1. Der Bund setzt sich dafür ein,
   - dass die Eidgenössischen Technischen Hochschulen, die Universitäten sowie die Fachhochschulen und Berufsbildungsinstitutionen mit Ausbildungsangeboten im Bereich der IKT die Informationssicherheit ausbauen und vernetzen und die dafür minimal notwendigen Lerninhalte festlegen;
   - dass die Informationssicherheit bei den Eidgenössischen Technischen Hochschulen, den Universitäten sowie den Fachhochschulen und Berufsbildungsinstitutionen Teil der Grundausbildung wird.

Sicherstellung einer zukunftssicheren kryptografischen Infrastruktur

2. Der Bund stellt in Zusammenarbeit mit den Kantonen sicher, dass die eingesetzte Verschlüsselungstechnik bei sensitiven Daten auch langfristig die notwendige Informationssicherheit gewährleistet. Die entsprechende Verschlüsselungstechnik soll allen privaten und öffentlichen Nutzerinnen und Nutzern zur Verfügung gestellt werden.

Sichere Kommunikationsinfrastruktur

3. Der Bund prüft in Zusammenarbeit mit den Kantonen die Möglichkeiten, privaten und öffentlichen Nutzerinnen und Nutzern ein sicheres und hoch verfügbares Kommunikationsnetzwerk zur Verfügung zu stellen.

Standards und Zertifizierungen bei Software und cyber-physischen Geräten und Schaffung von gesetzlichen Rahmenbedingungen

4. Der Bund prüft in Abstimmung mit der Entwicklung im Ausland, ob und in welchen Bereichen Standards und Zertifizierungen zu einer Voraussetzung für den Marktzugang von IKT-Komponenten erklärt werden müssen, und welche gesetzlichen Rahmenbedingungen dafür nötig sind.

Sichere digitale Identitäten

5. Der Bund schafft die notwendigen gesetzlichen Grundlagen für sichere staatlich anerkannte digitale Identitäten (für juristische und natürliche Personen sowie digitale Infrastrukturen).

6. Der Bund prüft die Möglichkeit, soweit Identifizierungen nicht notwendig sind, anonyme Anmeldenachweise („anonymous Credentials“) einzuführen, insbesondere für die Beziehungen zwischen Privaten und Behörden, aber auch als Mittel für die Online-Nutzer.

Aufbau eines nationalen Netzwerks zur Förderung der Forschung und des Wissenstransfers im Bereich der Informationssicherheit

7. Der Bund sorgt für die Schaffung eines nationalen Netzwerks zur Förderung der

Forschung im Bereich der digitalen Transformation mit Schwerpunkt Informationssicherheit und des Wissenstransfers zwischen der Forschung und der Wirtschaft.

Analysefeld Business to Consumer (B2C)

Schutz der Privatsphäre und der informationellen Selbstbestimmung

8. Der Bund setzt sich für eine Stärkung der informationellen Selbstbestimmung ein, fördert namentlich datenschutzfreundliche Technologien und prüft unter Berücksichtigung der internationalen Entwicklungen und des technischen Fortschritts ergänzende und alternative Ansätze inner- und ausserhalb des Datenschutzrechts.
9. Der Bund prüft, ob die geltenden Strafnormen ausreichen, um bei der Verletzung von Geheimnissen durch digitale Systeme (z.B. durch personalisierte Applikationen) den Verursacher zur Verantwortung ziehen zu können.
10. Bund und Kantone passen die Ausstattung der Datenschutzbehörden mit Befugnissen und Mitteln so an, dass diese es ihnen ermöglichen, ihre gesetzlichen Aufgaben der Sensibilisierung, Beratung und Aufsicht umfassend und wirkungsvoll wahrnehmen zu können.
11. Der Bund schafft in Zusammenarbeit mit den Kantonen Kooperationsformen zwischen den Datenschutzaufsichtsbehörden (z.B. Kompetenzzentrum).
12. Der Bund prüft mit Blick auf den Datenschutz und die Datensicherheit in Übereinstimmung mit den internationalen Entwicklungen und unter Berücksichtigung des Risikopotenzials und der Einsatzgebiete datenschutzkonforme Voreinstellungen.

Online-Geschäftsbedingungen

13. Der Bund setzt sich in Zusammenarbeit mit der Wirtschaft für die Einführung von Instrumenten ein, die zum Ziel haben, im Zusammenhang mit Online-AGB einen angemessenen Konsumentenschutz zu gewährleisten.

Online-Widerrufsrecht

14. Der Bund prüft die Frage, ob ein angemessenes Widerrufsrecht bei Online-Geschäften einzuführen ist.

Digitale Verträge und digitale Inhalte

15. Der Bund prüft für digitale Verträge und Inhalte unter Berücksichtigung der internationalen Entwicklungen, ob Anpassungen im Vertragsrecht nötig sind.

Preisdifferenzierung

16. Der Bund prüft, ob mittelfristig sektorspezifische Regulierungen, z.B. im Wettbewerbsrecht (UWG), in der Preisbekanntgabeverordnung oder im Versicherungsrecht nötig sind.

Online-Streiterledigung

17. Der Bund fördert Online-Beschwerde- und -Streitschlichtungsmechanismen (Online Dispute Resolution, ODR), unter Einbezug privater Angebote.

Analysefeld Business to Business (B2B)

Kartellrecht

18. Der Bund prüft im Kartellrecht, ob nicht alternativ zu den Umsatzschwellenwerten auch die Transaktionswerte geeignete Aufgreifkriterien bei der Prüfung von Unternehmenszusammenschlüssen wären.
19. Der Bund prüft unter Berücksichtigung der internationalen Entwicklungen, ob das Risiko einer durch Preisalgorithmen verursachten Kollusion im Kartellgesetz präziser geregelt werden soll.

B2C und B2B übergreifende Analysefelder: Datenzugang, Dateneigentum und neue Haftungsfragen

Zugang zu Sachdaten

20. Der Bund prüft die Ausgestaltung eines Zwangslizenzen-Systems mit Blick auf den Zugang zu Sachdaten.

Portabilität von Personendaten

21. Der Bund ergänzt unter Berücksichtigung der internationalen Entwicklungen das Datenschutzrecht um das Element der Datenportabilität.

Portabilität von Sachdaten

22. Der Bund prüft unter Berücksichtigung der internationalen Entwicklungen eine Regelung der Portabilität von Sachdaten.

Rechte an Daten

23. Der Bund schliesst Lücken betreffend die Rechte der Betroffenen beim Rechtsschutz, insbesondere durch Anpassungen des Bundesgesetzes über Schuldbetreibung und Konkurs und des Erbrechts.

Haftungsfragen

24. Der Bund prüft unter Berücksichtigung der internationalen Entwicklungen, insbesondere derjenigen in der EU, den Handlungsbedarf im ausservertraglichen Haftungsrecht (Produktehaftung, Produktesicherheit, Providerhaftung, Netzwerkinfrastrukturhaftung) und die allfällige Einführung neuer Haftungskonzepte.

Analysefeld Government to Citizen/Business (G2Ci/B)

Standards, Normen, Massnahmen der guten Praxis im Bereich der kritischen Infrastrukturen

25. Bund und Kantone erarbeiten in enger Zusammenarbeit mit den Fachverbänden auditierbare IKT-Sicherheitsstandards und verpflichten die Betreiber kritischer Infrastrukturen, diese Sicherheitsstandards zu beachten.

26. Der Bund baut ein Kompetenzzentrum (bzw. eine Stelle im Rahmen eines Kompetenzzentrums für Cybersicherheit) zu Fragen der Standardisierung im Bereich IKT-Sicherheit auf.

Standards, Normen, Massnahmen der guten Praxis in der breiten Wirtschaft

27. Der Bundesrat fördert in enger Zusammenarbeit mit den Dach- und Branchenverbänden, mit den Verbänden der IKT-Anbieter und mit interessierten Unternehmen Programme zur Verbesserung der Informationssicherheit in der Wirtschaft.

Meldepflichten

28. Der Bund führt für die Betreiber kritischer Infrastrukturen eine Meldepflicht für Cybervorfälle ein. Er erarbeitet dabei zusammen mit den zuständigen Behörden, der Privatwirtschaft und den Verbänden die Grundlagen und berücksichtigt die internationale Entwicklung.

Landesweite und zentrale Organisation zur Bewältigung von Cybervorfällen

29. Der Bund sorgt in Zusammenarbeit mit den Kantonen, der Wirtschaft und den Forschungsinstituten dafür, dass mit dem Ausbau von MELANI ein landesweites Zentrum (bzw. eine Stelle im Rahmen eines Kompetenzzentrums für Cybersicherheit, s. Empfehlung 26) zur Prävention und Bewältigung von Cybervorfällen geschaffen wird.

Betriebssicherheitsverfahren für die Betreiber kritischer Infrastrukturen und weitere Anspruchsgruppen

30. Der Bund prüft,
    - ob Betreiber kritischer Infrastrukturen eine Betriebssicherheitserklärung vorweisen müssen;
    - ob und wie das Betriebssicherheitsverfahren auch Stellen ausserhalb des Bundes und der Verwaltung bei sensitiven Beschaffungen zur Verfügung gestellt werden kann.

Grenzen staatlicher Abwehrmöglichkeiten

31. Der Bund führt eine sicherheitspolitische Diskussion im Bereich Cybersicherheit darüber, ob und in welchem Umfang eigene Abwehrressourcen aufzubauen und/oder enge Kooperationen mit anderen Staaten einzugehen sind. Im Vordergrund soll dabei die Cyberresilienz stehen.

Aufgaben der Armee

32. Der Bund trifft die nötigen Vorkehrungen, damit die Armee und die Militärverwaltung den zivilen Behörden subsidiär Mittel im Cyberbereich zur Verfügung

stellen können. Diese sollen in ausserordentlichen Lagen die Betreiber kritischer Infrastrukturen unterstützen können.

33. Der Bund präzisiert die Kriterien für den verhältnismässigen Einsatz der Armee im Cyberbereich.

Schweizweite Harmonisierung des Datenschutzes für die Verwaltung

34. Der Bund prüft zusammen mit den Kantonen eine Harmonisierung des öffentlich-rechtlichen Datenschutzes in der Schweiz.

Staat als Dienstleister

35. Bund und Kantone schaffen für die digitale Transformation im Bereich der Behördentätigkeiten medienbruchfreie und einheitliche Rahmenbedingungen, die eine auch für Private und Wirtschaft möglichst benutzerfreundliche sowie gut koordinierte und vernetzte Datenbearbeitung unter Wahrung des Datenschutzes ermöglichen und, wo es sinnvoll erscheint, Lösungen schweizweit skalieren lassen.

36. Bund und Kantone stellen sicher, dass bei der Umsetzung der E-Government-Strategie Schweiz die Bevölkerungsgruppe der „Offliner“ durch die Digitalisierung nicht gesellschaftlich ausgegrenzt wird.

Open Government Data (OGD) und Open Data

37. Bund und Kantone schaffen die gesetzlichen Voraussetzungen, damit die mit öffentlichen Mitteln erhobenen Daten unter Wahrung der datenschutzrechtlichen Vorgaben für die weitere Verwendung erschlossen werden können.

38. Bund und Kantone richten eine Fachstelle ein, die Standardisierungen und Normierungen auf der technischen und operativen Ebene bei der Datenbearbeitung im Bereich OGD erarbeitet und alle betroffenen Verwaltungsstellen fachlich unterstützt.

Digitalisierte Demokratie

39. Bund, Kantone und Gemeinden treffen geeignete Massnahmen, um Pilotprojekte mit innovativen Ansätzen der partizipativen Demokratie wie „Massive Open Online Deliberation“ zu fördern und Grundlagen für deren Beurteilung zu schaffen.

40. Bund, Kantone und Gemeinden fördern offene und partizipative Systeme und Prozesse (z.B. Open Data, Open Access, Open Science, Open Innovation, Citizen Science, Hackathons, Fablabs, Makerspaces, Gov Labs und City Challenges), um gesellschaftliche Ziele wie digitale Transformation, Resilienz und Nachhaltigkeit schneller zu erreichen.

41. Bund und Kantone dehnen E-Voting-Projekte nur aus, wenn aufgezeigt werden kann, dass E-Voting nicht mit grösseren Risiken verbunden ist als die bestehenden Formen der demokratischen Mitwirkung bei Wahlen und Abstimmungen. Wahl- und Abstimmungsergebnisse müssen überprüfbar bleiben.

Analysefeld Blockchain

42. Bund und Kantone stellen sicher, dass Blockchain-Lösungen bei sensitiven Anwendungen in der Verwaltung und in regulierten Bereichen nur dann zur Anwendung kommen, wenn eine langfristige Sicherheit (z.B. rechtzeitige Aktualisierungen) gewährleistet ist.
43. Der Bund nimmt, unter Berücksichtigung der regulatorischen Entwicklungen im Ausland, die nötigen rechtlichen Anpassungen bei der Behandlung von digitalen „Datenpaketen“ (Tokens), von digital geführten Registern und im Bereich des Datenschutzes vor.

Analysefeld Digitale Aufklärung der Bevölkerung, Kompetenzaufbau, Mitgestaltung des Nutzers und Forschung

Obligatorische Schule, Allgemeinbildung bis Tertiärstufe und Hochschulen

44. Bund und Kantone sorgen dafür, dass die Schülerinnen und Schüler im Rahmen der obligatorischen Schule und alle Studierenden die notwendigen Grundfertigkeiten und Kompetenzen für den Umgang und die Gestaltung mit digitalen Technologien und der Transformation entwickeln.

Berufliche Weiterbildung

45. Bund und Kantone schaffen in enger Zusammenarbeit mit allen betroffenen Kreisen der Gesellschaft und Wirtschaft die strukturellen Voraussetzungen, um die Weiterbildung für Berufsleute aller Bereiche zwecks Bewältigung der digitalen Transformation zu erleichtern.

Massnahmen für die Öffentlichkeit oder die Kultur

46. Bund und Kantone setzen sich für eine Kulturförderung ein, die sich verstärkt mit dem digitalen Wandel auseinandersetzt, und schaffen öffentliche Räume für den kreativen Umgang mit digitalen Technologien.

Analysefeld Digitale Transformation und Ethik

47. Bund und Kantone setzen sich dafür ein, dass der Schutz von Grundwerten, Menschenrechten und Menschenwürde auch im digitalen Zeitalter gesichert und die informationelle Selbstbestimmung gefördert werden.
48. Bund und Kantone sorgen in Zusammenarbeit mit den verantwortlichen Behörden und Anbietern im Bereich der Berufsausbildung dafür, dass die Ethik zu einem festen Bestandteil der Aus- und Weiterbildung wird, und nehmen diese Aspekte in ihre Erwartungen an das verantwortungsvolle Unternehmertum auf.
49. Bund und Kantone schaffen die Voraussetzungen dafür, dass Hochschulen und Weiterbildungseinrichtungen Forschung und Lehre in den Bereichen „Responsible Innovation“ (verantwortungsvolle Innovation) und „Design for Values“ (Werte-orientiertes Design) intensivieren.

50. Der Bund sorgt für ausreichende Transparenz, Nachvollziehbarkeit, Verständlichkeit und Accountability (Rechenschaftspflicht) bei digitalen Prozessen und Algorithmen, um eine vertrauensbasierte digitale Wirtschaft und Gesellschaft zu gewährleisten.

51. Der Bund schafft die nötigen rechtlichen Grundlagen, um sicherzustellen, dass bei elektronischer interaktiver Kommunikation transparent gemacht wird, wenn die Kommunikation nicht mit einem Menschen erfolgt.

Inhaltsverzeichnis

Vorbemerkung zur Sprache in diesem Bericht: Aus Gründen der Lesbarkeit wird gelegentlich auf geschlechtergerechtes Formulieren verzichtet. Damit die Lektüre des viele technische Begriffe enthaltenden Textes erleichtert wird, wurde ein Abkürzungsverzeichnis und Glossar mit Fachbegriffen erstellt (Beilage 3).

1 Einführung

1.1 Ausgangslage

Am 26. September 2013 reichte Ständerat Paul Rechsteiner die Motion 13.3841 „Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit“ ein.

Mit der Motion wurde der Bundesrat beauftragt, eine interdisziplinäre Expertenkommission einzuberufen und folgenden Fragen nachzugehen:

1. Wie sind die technologischen und politischen Entwicklungen auf dem Gebiet der Datenbearbeitung zu beurteilen?
2. Was bedeuten diese Entwicklungen für die schweizerische Wirtschaft, die Gesellschaft und den Staat?
3. Wie ist der gegenwärtige Rechtsrahmen mit Blick auf diese Entwicklung zu beurteilen?
4. Welche Empfehlungen ergeben sich daraus für die Schweiz? Auf nationaler Ebene? Mit Blick auf mögliche Initiativen auf internationaler Ebene?

Begründung des Motionärs:

Die Enthüllungen von Edward Snowden zeigen, dass die Grundannahmen, von denen auch in der Schweiz auf dem Gebiet der Datenbearbeitung und Datensicherheit ausgegangen wurde, nicht mehr zutreffen. Zwar übersteigen die Dimensionen der aufgeworfenen Probleme die schweizerischen Grenzen bei Weitem. Trotzdem ist die Schweiz als wirtschaftlich hochentwickeltes Land gut beraten, sich ein eigenes Bild zu machen. Dazu bedarf es – vor allfälligen Schlussfolgerungen – der qualifizierten Beurteilung geeigneter Experten.

Beratung in den eidgenössischen Räten:

National- und Ständerat betonten, dass die Vorkehrungen des Bundesrates, insbesondere die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken, einen ersten wichtigen Schritt darstellen. Allerdings würden diese Arbeiten hauptsächlich auf den Schutz des Staates und der kritischen Infrastrukturen fokussieren. Die Bedeutung der digitalen Entwicklung für die Schweizer Gesellschaft als Ganzes, die Bevölkerung und die Wirtschaft würden nur unzureichend berücksichtigt. Eine Expertenkommission könne diesen für die digitale Zukunft der Schweiz wichtigen Fragen nachgehen und der Bericht eine öffentliche Debatte ermöglichen.

Die Motion wurde im Ständerat am 3. Dezember 2013 angenommen, im Nationalrat mit einer Ergänzung am 13. März 2014.

1.2 Zusammensetzung der Expertengruppe

Das mit der Umsetzung der Motion beauftragte Eidgenössische Finanzdepartement setzte die Kommission aus formalen Gründen als Expertengruppe ein. Diese setzte sich aus zwölf Expertinnen und Experten aus Wissenschaft, Verwaltung und Wirtschaft zusammen. Die Liste der Mitglieder der Expertengruppe findet sich in der Beilage 1. Als Präsidentin wurde alt Nationalrätin Brigitta M. Gadient berufen. Das EFD siedelte die Expertengruppe im Generalsekretariat an. Die Arbeit der Expertengruppe wurde auf maximal drei Jahre bis 2018 befristet.

1.3 Themenschwerpunkte und Abgrenzung

Angesichts der Themenbreite und begrenzter Ressourcen legte die Expertengruppe den Schwerpunkt auf die Informationssicherheit, den Datenschutz, Haftungsfragen, den Zugang zu Daten und die Besitzverhältnisse an Daten.

Die Analysefelder „Digitale Aufklärung der Bevölkerung, Kompetenzaufbau, Mitgestaltung des Nutzers und Forschung“ sowie „Digitale Transformation und Ethik“ wurden so weit verfolgt, wie die Erarbeitung einer Diskussionsgrundlage und die Formulierung genereller Empfehlungen es verlangte. Im Bereich G2Ci/B (Government to Citizen/Business) standen die Bereiche Schutzaufgaben des Staates, OGD (Open Government Data) und E-Government im Mittelpunkt. Den sozioökonomischen Folgen der digitalen Transformation (Folgen für den Arbeitsmarkt, Gig Economy, etc.) mit ihren insbesondere sozial-, arbeits- und steuerrechtlichen Aspekten ist die Expertengruppe nur am Rande nachgegangen. Ebenso hat sie darauf verzichtet, die Folgen der digitalen Transformation in der Finanzwirtschaft zu erörtern, sofern diese nicht Sicherheitsfragen und das Phänomen Blockchain berührten.

Im Rahmen des RUAG-Vorfalls im Frühjahr 2016 erhielt die Expertengruppe zudem den Auftrag, die Gegenmassnahmen des Bundesrates zu prüfen und bis Ende 2016 einen diesbezüglichen Bericht zu verfassen.

1.4 Vorgehen und Aufbau des Berichts

Das einführende Kapitel (s. Ziff. 3) hält aus genereller Sicht die Eckpfeiler der heutigen Entwicklung fest und analysiert deren Push- und Pull- Faktoren sowie die Chancen und Risiken. In einem zweiten Schritt werden in den Kapiteln vier bis elf die einzelnen Analysefelder auf den Ist-Zustand, die weitere Entwicklung, die Chancen und Risiken, den Ordnungsrahmen (Regularien) und den kurz- bzw. langfristigen Handlungsbedarf untersucht. Bei den Empfehlungen geht die Expertengruppe von den folgenden übergeordneten Zielen aus:

- Sicherstellung der Menschenwürde und der Persönlichkeitsrechte bzw. des Persönlichkeitsschutzes;
- Sicherstellung der digitalen Entwicklungsmöglichkeiten aus gesamtgesellschaftlicher Sicht;
- Sicherstellung der staatlichen Handlungsfähigkeit;
- Sicherstellung des Konsumentenschutzes;
- Sicherstellung einer umsetzbaren Informationssicherheit für die verschiedenen Akteure in den verschiedenen Wirtschaftssektoren, für den Staat und für die private Nutzerin bzw. den privaten Nutzer.

Für die umfangreichen Abklärungsarbeiten wurden Subarbeitsgruppen eingesetzt. Eine zusätzliche Arbeitsgruppe wurde für die Umsetzung des RUAG-Auftrags gebildet. Dieser Bericht zuhanden des Bundesrates floss nicht in den Schlussbericht der Expertengruppe ein.

Die Subarbeitsgruppen zogen verschiedentlich weitere Fachexpertinnen und -experten bei bzw. führten Anhörungen mit Experten durch, insbesondere in den Bereichen Forschung, Bildung und Sensibilisierung sowie im Bereich IKT-Sicherheit und Risikomanagement zur Erarbeitung eines allfälligen IKT-Grundschutzes für die breite Wirtschaft.

1.5 Anhörungen von Interessenvertretern, Expertinnen und Experten

Um die Bedürfnisse und Anliegen der unterschiedlichen Interessenvertreter und Wirtschaftszweige einzubeziehen, wurden verschiedene Anhörungen durchgeführt. Für weitere Anhörungen wurden Fachexperten eingeladen (s. Liste Beilage 2).

2 Auftragsanalyse

2.1 Definition des Untersuchungsgegenstands

Die Entwicklung der elektronischen Informations- und Kommunikationstechnologie hat zu einer digitalen Durchdringung aller Lebensbereiche geführt; Wirtschaft, Gesellschaft, Staat und die grosse Mehrheit der Personen sind gleichermassen davon betroffen. Ausdruck dieser Digitalisierung ist die digitale Erfassung und Vermessung der Welt, wobei in der Regel analoge Werte in elektronische Daten verwandelt, weiterbearbeitet und dann gespeichert werden. Die Grundeinheit der sogenannten „digitalen Revolution“ sind Daten – unabhängig davon, ob es sich nun um Sach- oder Personendaten, Steuerungsdaten, Informationsdaten, Überwachungsdaten, Kommunikationsdaten usw. handelt.

Eindrücklich an dieser Entwicklung sind zum einen die Menge der Daten, zum anderen deren Vernetzbarkeit, deren Auswertbarkeit durch neue Analyseinstrumente und die Tatsache, dass es kaum noch Bereiche der realen Welt gibt, die nicht davon betroffen sind. Waren es früher nur Computer, sind es heute im Wesentlichen mobile Endgeräte und vernetzte Dinge (Internet of Things, IoT), die zu einem exponentiellen Anstieg der Datenmenge führen.

Der technologische Fortschritt hat die Grundlagen für diese Entwicklung gelegt. Ein wesentlicher Treiber dieser digitalen Transformation war und ist aber die Wirtschaft. Eine Vielzahl von digitalen Infrastrukturen und Diensten steht allen, überall und rund um die Uhr zur Verfügung und prägt alle Lebensbereiche. In erster Linie wären zu nennen: Soziale Medien, Online-Shopping, Online-Gaming, Big Data, Internet of Things (IoT), Algorithmen und Vorformen der künstlichen Intelligenz (Machine Learning, Deep Learning), Blockchain, Virtual Reality und Augmented Reality, Social und Chat Bots. Neue digitale Infrastrukturen wie Quantencomputer, ausgeklügelte Mensch-Maschinen-Schnittstellen stehen davor, ein kommerzialisierbares Entwicklungsniveau zu erreichen. Entsprechend gross ist das wirtschaftliche Potenzial. Basisstoff dieser Entwicklung wird die Datenbearbeitung bleiben. Daher hat die Expertengruppe die erste Frage der Motion nach der technischen und politischen Entwicklung um den wirtschaftlichen Aspekt erweitert.

Neben den vielen Vorteilen der modernen Datenbearbeitung und der digitalen Transformation wie Produktivitäts- und Effizienzgewinne, neue Dienstleistungen, Komfort, neue Möglichkeiten der Zusammenarbeit (Crowdfunding, -sourcing, -knowledge), die Chance, aus einer Informationsgesellschaft eine Wissensgesellschaft zu formen und eine Demokratisierung des Wissens zu erreichen, lassen sich auch Risiken nicht übersehen. Die Herausforderungen der Datenbearbeitung stellen sich wie folgt dar:

1. Was sind Daten aus rechtlicher Sicht? Informationsträger oder Wertgüter? Wer darf sie wann erfassen, weiterverarbeiten, übernehmen, verwerten, nutzen, sein Eigentum nennen, kopieren oder als geistiges Eigentum definieren?
2. Die Entwicklung der Datenbearbeitung hat erhebliche Auswirkungen auf den Schutz der Privatsphäre und der informationellen Selbstbestimmung. Dabei geht es um grundlegende Menschenrechte wie den Persönlichkeitsschutz, die Wahrung der eigenen Handlungsfähigkeit und auch das Recht, in Ruhe gelassen zu werden. Die digitale Transformation stellt für diese Prinzipien und Grundwerte eine Herausforderung dar: Es entstehen neue Spannungsfelder zwischen IKT-Sicherheit und Benutzerkomfort, Eigenverantwortung und Konsumentenschutz,

minimiertem Transaktionsaufwand und Datenschutzauflagen. Vor diesem Hintergrund müssen Anbieter, Nutzer, Konsumenten und der Staat die bisherigen Zusammenarbeits- und Vertrauensverhältnisse neu aushandeln und allenfalls neu definieren.

3. Bei einer sicheren Datenbearbeitung geht es um technische und organisatorische Fragen wie Gewinnung, Verarbeitung, Transport, Speicherung und Archivierung von Daten. Dabei sind alle vier Attribute der IKT-Sicherheit d.h. Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit als Grundvoraussetzungen für eine Datensouveränität zu berücksichtigen.
4. Die Digitalisierung hat zu einer Vielzahl von neuen Geschäftsmodellen geführt – einige wie die Verlagerung der Werbung ins Internet waren disruptiv. Es ist davon auszugehen, dass disruptive Phänomene zunehmen werden. Dies stellt eine Vielzahl bisheriger Ordnungsstrukturen wie etwa den Konsumentenschutz, das Arbeitsrecht, das Sozialversicherungsrecht, das Steuerrecht, das Immaterialgüterrecht und das Wettbewerbsrecht vor bedeutende Herausforderungen.
5. Die Macht der Kontrolle über die Daten und die Informationsflüsse hat nicht nur Auswirkungen auf die Souveränität des Einzelnen, sondern auch auf die Souveränität der gesamten Gesellschaft, ihre Kohäsion und ihre demokratischen Strukturen. Technisch gesehen gehen bereits heute die Möglichkeiten der Überwachung und Manipulation weit über das hinaus, was George Orwells dystopischer Roman „1984" skizziert hat. Das Risiko des Missbrauchs ist zu minimieren.
6. Die Folgen der digitalen Transformation auf die Datenbearbeitung gehen über rein sicherheitstechnische, rechtliche oder regulatorische Fragen hinaus. Die Entwicklung hat eine Stufe erreicht, auf der historisch gewachsene Wertestrukturen und Rechtsprinzipien der Gesellschaft in Frage gestellt werden. Deshalb spielen ethische Aspekte für die Beantwortung dieser grundlegenden Fragen eine entscheidende Rolle.

Für die einen ist die digitale Revolution der perfekte Sturm, der sich zusammenbraut, für die anderen die Chance für den nächsten Entwicklungsschritt der Gesellschaft. Wie bei jeder grösseren technischen Entwicklung liegen Risiken und Chancen eng beieinander. Deren Beurteilung wurde in den einzelnen Analysefeldern gleichermassen Rechnung getragen.

2.2 Analysefelder

Der Einbezug der gesamtgesellschaftlichen Dimension spielte in den Erwägungen des Parlamentes zur Motion eine mitentscheidende Rolle. Aus diesem Grund wählte die Expertengruppe eine Querschnittsperspektive aus, welche die ganze Vielfalt der verschiedenen Datentypen und Infrastrukturen sowie alle betroffenen Gesellschaftsakteure berücksichtigt.

Für die Diskussion der gesamtgesellschaftlichen Dimension definierte die Expertengruppe drei Analysefelder, in denen die Beziehungen der Akteursgruppen (Bürger, Konsumenten, Anbieter, Produzenten, Behörden) untereinander im Zentrum stehen. Die drei akteurbezogenen Analysefelder sind:

- Anbieter/Produzenten im Verhältnis zum Konsumenten und Nutzer (B2C);
- Anbieter und Produzenten untereinander (B2B);
- der Staat im Verhältnis zum Bürger und zur Wirtschaft (G2Ci/Business).

Weitere fünf Analysefelder haben einen thematischen Querschnittscharakter: „Informationssicherheit“, „Datenzugang und Datenportabilität“, „Blockchain“, „Digitale Aufklärung der Bevölkerung, Kompetenzaufbau, Mitgestaltung des Nutzers und Forschung" sowie „Digitale Transformation und Ethik“.

Dieser Ansatz erlaubte im Hinblick auf die Fragestellung 3 der Motion eine die einzelnen relevanten Rechtsgebiete übergreifende Überprüfung und Beurteilung.

2.2.1 Analysefeld Informationssicherheit

Für eine ganzheitliche Betrachtung muss die Datensicherheit in einen breiten Kontext gestellt werden. Aus diesem Grund wird im Folgenden der weitergefasste Begriff Informationssicherheit verwendet, allerdings mit der Einschränkung, dass weiterhin die digitale Information im Vordergrund steht. Da die digitalen Infrastrukturen – vom Smartphone bis hin zum Ökosystem Internet – die Basis für die heutige Datenbearbeitung darstellen, hängen die Sicherheit und die Resilienz der Daten wesentlich von der Sicherheit und Resilienz dieser digitalen Infrastrukturen ab.

Im Analysefeld „Informationssicherheit“ wurden die Bedrohungen, die Gefahren, das allfällige Schadenspotenzial, die Angriffsfläche und die Chancen für die digitalen Infrastrukturen erörtert. Die Expertengruppe führte eine Standortbestimmung durch, wie es um die Informationssicherheit steht, diskutierte die weitere Entwicklung und die Herausforderungen und zeigte Lösungsansätze auf.

Die Themen reichen dabei vom Dilemma zwischen Bedienungskomfort und Sicherheit über die Herausforderung Komplexität und fehlende Industrialisierung der IKT-Sicherheit bis hin zu den Chancen, aber vor allem auch den Risiken der technologiegetriebenen Kultur, Verwaltung und Wirtschaft, in denen das „Technisch-Machbare“ das „Sicher-Umsetzbare“ permanent herausfordert. Schliesslich geht es um die Folgen für die analoge Welt, die je länger desto mehr von dieser Datenbearbeitung gesteuert wird.

Die Expertengruppe ging der grundlegenden Frage nach, was überhaupt Sicherheit in der digitalen Welt bedeutet. Ist Sicherheit im digitalen Umfeld messbar und fassbar? Ist eine Metrik vorhanden, die ein effizientes und erfolgreiches Risikomanagement erlaubt?

Neben Fragen der Aus- und Weiterbildung im Bereich IKT-Sicherheit für IKT-Expertinnen und -Experten, für betroffene Berufsfelder und die breite Bevölkerung wurden schliesslich folgende Themen vertieft behandelt: die Kryptografie, die sichere Authentifizierung und Identifizierung in der digitalen Welt, die Frage nach der Notwendigkeit von Normen und Standards bei Organisationen und Produkten insbesondere in der vernetzten Welt der Dinge (IoT) und der Bedarf nach einem sicheren Kommunikationsnetzwerk für die Schweiz.

2.2.2 Analysefeld Business to Consumer (B2C)

Im Analysefeld B2C stehen die Kundinnen und Kunden sowie die Nutzerinnen und Nutzer im Fokus. Internet und neue Geschäftsmodelle haben die Abhängigkeits-, Wissens - und Machtverhältnisse zwischen Datenherren und Datenbearbeitern einerseits und den Anbietern und Konsumenten andererseits verändert. Dies hat Auswirkungen auf den Schutz der Privatsphäre und der informationellen Selbstbestimmung wie auch auf den Konsumentenschutz.

Die erhobene Datenmenge über die Kunden und Nutzer sowie die Datenverdichtung fordern die heutigen Prinzipien der informationellen Selbstbestimmung und den Schutz

der Privatsphäre zunehmend heraus. Angesichts dieser Entwicklung und der Tatsache, dass das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG) in Revision steht, ging die Expertengruppe den Fragen nach, ob der traditionelle Datenschutz und dessen konsequente Weiterentwicklung im Rahmen der oben genannten Revisionsarbeiten (E-DSG) auch in Zukunft diesen Herausforderungen gerecht werden können, ob es Alternativen gibt und wo diese ansetzen könnten. Im Mittelpunkt steht die Frage, inwiefern die Prinzipien des Datenschutzes mit den modernen Methoden der Datenbearbeitung wie Big Data Analysen und künstliche Intelligenz (KI) in einem Spannungsverhältnis stehen. Hierzu hat die Expertengruppe mit Entwicklungsszenarien gearbeitet, die auch einen längerfristigen Zeithorizont abdecken.

Das Erfassen der Nutzer und Kunden durch Profiling und Scoring führt zu neuen Herausforderungen im Konsumentenschutz wie etwa einer intransparenten und diskriminierenden Preisdifferenzierung und Angebotsgestaltung. Ebenso ist nicht zu übersehen, dass bei sozialen Netzwerken dem Nutzer der Wechsel zu Alternativen erschwert und die Transaktionsaufwendungen erhöht werden. Vor diesem Hintergrund ist die Expertengruppe verschiedenen Teilaspekten des Konsumentenschutzes wie „Online Geschäftsbedingungen“, Preisdifferenzierung, Aspekten der Vertragsregelung im digitalen Bereich, Zugangssperren und Geoblocking nachgegangen. Die in diesem Zusammenhang auch wichtige Frage nach der Haftung wird im Analysefeld „B2C und B2B übergreifende Analysefelder: Dateneigentum, Zugang zu Daten und neue Haftungsfragen“ behandelt (s. Ziff. 2.2.4 und 7).

2.2.3 Analysefeld Business to Business (B2B)

Im Zuge der digitalen Transformation zeigen sich die Folgen der internationalen Vernetzung besonders ausgeprägt im Analysefeld B2B. Einleitend diskutierte die Expertengruppe im Analysefeld B2B die Auswirkungen der sogenannten „Sharing Economy“. Diese Entwicklung führt zu neuen Geschäftsmodellen, wobei die Grenze zwischen privaten und unternehmerischen Anbietern von Dienstleistungen und Produkten immer durchlässiger wird. Im Bereich der Sharing Economy beschränkte sich die Expertengruppe darauf, allgemein den Regelungsbedarf neuer Geschäftsmodelle, wie Beherbergungsplattformen und Mobilitätsdienstleistungen, zu identifizieren. Spezifische Rechtsbereiche wie das Arbeits-, Sozialversicherungs-, Steuer-, Mietrecht usw. wurden nicht detailliert behandelt, da verschiedene Bundesämter im Auftrag des Bundesrates in diesem Bereich bereits Abklärungen an die Hand genommen haben (u.a. SECO und ASTRA).

In einem zweiten Gebiet wurde das Augenmerk auf das Verhältnis der Unternehmen untereinander ausgerichtet. Im Kontext der neuen digitalen Online-Märkte stehen hierbei insbesondere das Kartellgesetz vom 6. Oktober 1995 (KG) sowie das Bundesgesetz vom 19. Dezember 1986 gegen den unlauteren Wettbewerb (UWG) im Fokus. Ferner wurden auch Aspekte der engen internationalen Vernetzung und deren möglichen rechtlichen Auswirkungen erläutert.

2.2.4 B2C und B2B übergreifende Themen: Dateneigentum, Zugang zu Daten, neue Haftungsfragen

Ein wesentlicher Aspekt der Datenbearbeitung betrifft die Frage, wie natürlichen und juristischen Personen die Rechtsposition verschafft werden kann, über ihre Daten (Sach- und Personendaten) zu verfügen. Dazu gehören Themen wie die Datenportabilität, der Zugang zu Daten und die Diskussion, welche Vor- und Nachteile ein Eigen-

tum an Daten mit sich brächte. Aus Sicht des Persönlichkeitsschutzes, des Konsumentenschutzes (B2C), aber auch der wirtschaftlichen Datenbearbeitung (B2B) ergeben sich vielerlei Probleme bezüglich der Übertragung von Gebrauchsrechten sowie der ausschliesslichen Nutzung und der Herausgabe von Daten. So erbringt bei diesem Fragenkomplex eine strikte Unterscheidung zwischen den Bereichen B2C und B2B keinen Nutzen mehr.

Die Digitalisierung führt zu neuen Haftungssituationen, die im weitesten Sinne meist einen Bezug zum Thema der Informationssicherheit aufweisen, aber sich inhaltlich auch auf neue Geschäftsmodelle auswirken. Anbieter sowie Nutzer von Dienstleistungen und Produkten sind gleichermassen von Haftungsfragen betroffen, unabhängig davon, ob es sich um Geschäfts- oder Privatkunden handelt. Deshalb hat die Expertengruppe auf eine gesonderte Betrachtung im Rahmen der Akteurverhältnisse B2C und B2B verzichtet.

2.2.5 Analysefeld Government to Citizen/Business (G2Ci/B)

Im Analysefeld „Government to Citizen/Business“ wird nicht nur in einem eng gefassten Sinn das Akteursverhältnis zwischen dem Staat und den Bürgerinnen und Bürgern beleuchtet, sondern auch in einem Multistakeholder-Ansatz das Verhältnis zwischen dem Staat und allen anderen Gesellschaftsteilnehmerinnen und -teilnehmern – von den Betreibern kritischer Infrastrukturen über die Privatwirtschaft und Organisationen bis hin zu privaten Personen.

Die Enthüllungen von Edward Snowden haben zur allgemeinen Erkenntnis und zum Bewusstsein geführt, dass Nachrichtendienste, weitere staatliche Behörden und staatsnahe Akteure die Digitalisierung und die neuen technischen Möglichkeiten dazu nutzen, flächendeckend und auf Vorrat Daten zu sammeln und Spionage zu betreiben. Diese Entwicklung ist einerseits eine Herausforderung für das Verhältnis zwischen dem Staat mit seinem Sicherheitsapparat und dem einzelnen Individuum mit seinem Recht auf Privatsphäre. Andererseits ist der Cyberraum eine Herausforderung für den Staat, seine Schutzaufgaben wahrzunehmen, entsprechende Unterstützungsleistungen für Gesellschaft und Wirtschaft zu definieren und angemessene Rahmenbedingungen zu schaffen.

Dazu gehören allgemeine Aspekte wie die Wahrung der digitalen Souveränität: Wie weit soll und kann der Staat das „Netz“ und die digitalen Infrastrukturen als erweiterten öffentlichen und privaten Raum betrachten, wo er seinen staatlichen Aufgaben (Schutz der Freiheit und Sicherheit, Chancengleichheit, Wohlfahrt, friedliche und gerechte Ordnung) nachkommen muss? Inwiefern soll der Staat (Bundesverwaltung, Kantone, Gemeinden) der Bürgerin oder dem Bürger digitale Dienstleistungen wie Cloud-Services oder andere IKT-Leistungen im Bereich der Sicherheit anbieten? Steigende Risiken sind auch bei den Lieferketten im IKT-Bereich auszumachen, wenn gewisse Länder ihre IKT-Industrie gesetzlich oder auf anderem Weg veranlassen können, vertraglich vereinbarte und/oder gesetzlich vorgeschriebene Geheimhaltungspflichten mit ihren Kunden nicht einzuhalten. Die Expertengruppe ging auch weiteren spezifischen Fragen nach wie: Sind Sicherheitsstandards und Normen im IKT-Bereich nötig? Braucht es Meldepflichten nach Cybervorfällen? Weiter erörtert das Kapitel G2Ci/B, wie der Staat landesweit die Bewältigung der Cybergefahr präventiv und reaktiv verbessern kann und welche Rolle dabei die Armee spielt.

Bei G2Ci/B geht es aber nicht nur um den Staat und seine Schutzaufgaben, sondern auch um seine Rolle als Anbieter staatlicher Dienste in digitaler Form (E-Government)

und als Förderer einer Open-Data-Kultur. Dazu gehören auch die Datenbestände des öffentlichen Sektors (Open Government Data, OGD).

Schliesslich beschäftigte sich die Expertengruppe sowohl mit den Chancen und Risiken als auch mit den Auswirkungen der digitalen Transformation im Kontext der bestehenden Demokratie: Welcher Stellenwert kommt allgemein den Medien sowie den grossen Internetanbietern im Staatsgefüge zu? Wie lassen sich neue, subtile, grossflächige Propaganda- und Zensurmöglichkeiten, wie sie mit der algorithmischen Steuerung von Newsfeeds in sozialen Medien („Big Nudging“ und „Social Bots“) entstehen, in demokratie-kompatible Bahnen lenken? Wie gross ist das Risiko der Manipulation? Wird hier das Recht verletzt, „in Ruhe gelassen zu werden“? Letztlich stellt sich die grundsätzliche Frage, wie aus einer potenziell manipulierbaren Informationsgesellschaft eine selbstbestimmte Wissensgesellschaft wird.

2.2.6 Analysefeld Blockchain

Die Blockchain-Technologie hat durch die verschiedenen digitalen Währungen, allen voran Bitcoins, grosse Aufmerksamkeit erlangt. Die Blockchain-Technologie, auch „distributed Ledger Technology“ (dt. verteilte Registerführung) genannt, bietet darüber hinaus eine Vielzahl von Anwendungsmöglichkeiten, wenn es darum geht, Transaktionen digital festzuhalten. Es ist davon auszugehen, dass der Blockchain in Zukunft eine bedeutende Rolle zukommen wird. Dies führte die Expertengruppe dazu, diese neue digitale Infrastruktur für die Datenbearbeitung gesondert zu betrachten und zwar aus rechtlicher und sicherheitstechnischer Sicht.

Blockchain führt zu neuen Chancen und Risiken. Zu nennen sind neue Finanzierungsmodelle und Möglichkeiten der Kapitalallokation ohne Intermediäre im Bereich des „initial Coin Offering“ (Fundraising über „Ledger Technology“) und digitale Geldsysteme mit niedrigeren Transaktionskosten. Allerdings sind die Anwendungen auch mit Risiken verbunden, wie etwa fehlender Transparenz, Rechtsunsicherheit, Geldwäscherei und einem möglichen Kontrollverlust des Staates über die Geldmenge und die transnationalen Geldflüsse. Diesen Risiken und Chancen im Finanzbereich konnte die Expertengruppe im Rahmen ihres begrenzten Auftrags nicht nachgehen.

2.2.7 Analysefeld Digitale Aufklärung der Bevölkerung, Kompetenzaufbau, Mitgestaltung des Nutzers und Forschung

In diesem Analysefeld identifizierte die Expertengruppe als vier zentrale Charakteristika der Digitalisierung:

- die beschleunigte Automatisierung zahlreicher Prozesse in der Arbeitswelt;
- die zunehmende digitale Vermessung aller Lebensbereiche;
- die durch digitale Technologien enorm gestiegene Möglichkeit, mediale Inhalte zu schaffen, zu verbreiten und zu verändern und
- die zunehmende Bedeutung und Abhängigkeit von autonomen Systemen.

Der Bildung kommt ein grosser Stellenwert zu, wenn es darum geht, diese Herausforderung anzupacken und die Bevölkerung dazu zu bringen, aktiv die Digitalisierung mit zu gestalten. Die Expertengruppe hat für jede Stufe bzw. all diese Bereiche überlegt, welche Veränderungen nötig sind. Mit der Bildung kommt auch den Kompetenzen ein grosser Stellenwert zu. Die Expertengruppe hat Empfehlungen formuliert, wie der Prozess ausgestaltet sein soll, um gefragte Kompetenzen zu identifizieren. Schliesslich

hört die Bildung nicht mit der obligatorischen Schule oder der beruflichen Erstausbildung auf. Es braucht vielmehr eine Gesellschaft, die lebenslang lernt. Neben der Bildung hat sich die Expertengruppe Gedanken dazu gemacht, wie die Kultur oder die generelle Öffentlichkeit dazu genutzt werden kann, die Bevölkerung für Themen der Digitalisierung zu sensibilisieren und zu befähigen.

2.2.8 Analysefeld Digitale Transformation und Ethik

Im Analysefeld „Digitale Transformation und Ethik“ diskutierte die Expertengruppe die Auswirkungen der Digitalisierung auf unsere Wertvorstellungen und damit zusammenhängende ethische Fragen. Einige der bereits in den anderen Analysefeldern angesprochenen, aber auch neu dazu kommende Probleme wurden dabei hinsichtlich ihrer Auswirkungen auf zentrale Werte wie Menschenwürde und Privatsphäre, Gleichheit und Diskriminierungsverbot, Autonomie und Selbstbestimmung sowie Transparenz, Solidarität und Sicherheit genauer analysiert. Diese ethische Analyse sollte dabei auch prüfen, inwieweit ethisches Denken sowohl unerwünschte Entwicklungen verhindern, als auch wünschbare Entwicklungen fördern kann.

Das Kapitel versucht dabei, die grundlegenden ethischen Herausforderungen der digitalen Transformation in der gebotenen Kürze darzustellen; dies im Wissen, dass die dabei angesprochenen Fragen eine weitaus tiefergehende Analyse erfordern würden. Es war der Expertengruppe deshalb stets bewusst, dass sie im besten Fall lediglich die Problemerfassung, Lösungsansätze und Empfehlungen skizzieren konnte. Ihr Ziel war hier, soweit möglich eine Grundlage für die notwendige Diskussion zu liefern; im Wissen, dass Ethik eine zentrale Grundlage für gesetzgeberische Arbeit und regulatorische Massnahmen bildet.

Die Expertengruppe setzte folgende Schwerpunkte:

- Wie kann primär sichergestellt werden, dass die Diskussion um Ethik nicht reaktiv hinter der Technik hinterherhinkt, sondern aktiv diese Entwicklung begleiten kann?
- Wie können werte-sensitive Ansätze (etwa „value-sensitive Design“) dazu beitragen, eine technologische Entwicklung zu gewährleisten, die mit den Grundwerten der Gesellschaft vereinbar ist?
- Wie kann sichergestellt werden, dass ethisches Denken einen angemessenen Stellenwert in der Aus- und Weiterbildung jener Fachpersonen einnehmen kann, welche die Digitalisierung massgeblich prägen?
- Mit welchen Massnahmen kann der Schutz der Grundwerte unserer Gesellschaft verbessert werden?

3 Eckpfeiler der heutigen Entwicklung

3.1 Push-Faktoren

3.1.1 Technische Voraussetzungen

Der wichtigste Push-Faktor war und ist die technologische Entwicklung. Einige der wichtigsten technischen Triebkräfte der allgegenwärtigen Digitalisierung wirken zwar bereits seit mehr als 50 Jahren: Dazu gehören die Rechenleistung von Prozessoren, die Stabilität und Geschwindigkeit der Datentransportnetze sowie die Möglichkeit, Daten zu erheben und zu speichern. Über Jahrzehnte war der Einfluss dieser Triebkräfte auf die Lebenswelt verhältnismässig gering, obwohl Computer im Büro, in der Produktion und im privaten Bereich zunehmend zur Anwendung kamen. In den letzten 15-20 Jahren erreichten diese Triebkräfte aber einen Entwicklungsstand und Kostengrad, der ihre vernetzte Massennutzung erlaubte und einen Schneeballeffekt auf die weitere Technologieentwicklung hatte.

3.1.1.1 Technologische Entwicklungen in Zahlen I: Die Rechenleistung der Computer

Die Entwicklung integrierter Schaltkreise in kommerziellen Computerchips ist ein Grundpfeiler der digitalen Revolution. Hatte ein Chip anfangs der 1970er-Jahre 2300 Transistoren (Intel 4004), sind heute auf einem Chip Milliarden von Transistoren platziert. Hätte die Geschwindigkeit der Autos in den letzten 40 Jahren im gleichen Ausmass zugenommen, wären unsere heutigen Personenfahrzeuge mit ca. einem Zehntel der Lichtgeschwindigkeit unterwegs. Jeder der rund drei Milliarden Smartphonebesitzer weltweit trägt heute einen Computer mit sich, der leistungsfähiger ist als die zimmergrossen Supercomputer aus den 1980er-Jahren. Das „Mooresche Gesetz“ aus dem Jahre 1965, nach dem sich die Anzahl Transistoren pro Fläche alle zwei Jahre verdoppeln würde, hat sich bewahrheitet. Allerdings nimmt die Rechengeschwindigkeit nicht so schnell zu wie die Möglichkeit zur Speicherung, die sich alle 18 Monate verdoppelt.

Allmählich stösst die Miniaturisierung der Chips aber an ihre Grenzen: Die Transistoren der 1970er-Jahre hatten die Grösse einer Blutzelle und waren mit einem Schulmikroskop zählbar, heute haben sie noch die Breite von 100 Atomen (ca. 20 nm, d.h. 20 Millionstel Millimeter), was die Steuerung der Ladungen immer schwieriger und die Produktion immer teurer macht. Das nahende Ende des Mooreschen Gesetzes hat aber bereits heute neue Entwicklungen angestossen: neue Transistorendesigns, neue Materialien, Quantencomputer und die Anwendung optimierter Chips für spezifische Zwecke in der Cloud. Die Vernetzung der Computer befreit den Endbenützer von der Leistungsfähigkeit seines eigenen Computers. Wenn heute das Navigationsgerät die schnellste Route berechnet, sendet es lediglich die Eckdaten. Die komplizierte Berechnung erfolgt in der „Cloud“ durch spezialisierte Hardware. Die meisten „App-Dienste“ beruhen genau auf diesem Prinzip – eine Entwicklung, die weiter zunehmen dürfte.

3.1.1.2 Technologische Entwicklungen in Zahlen II: Die Vernetzung der Computer

Die Vernetzung der Computer ist der zweite Grundpfeiler der Digitalisierung. Ohne den revolutionären Fortschritt bei der Datenübertragung bezüglich Kapazität und Qualität

wäre die bisherige Entwicklung nicht möglich gewesen. 1977 hatte das erste moderne Modem eine Übertragungsrate von 300 Bits pro Sekunde, was ca. 37 Buchstaben entspricht. Der heutige Mobilfunkstandard LTE ermöglicht theoretische Übertragungsraten von 300 Mbit/s (300 000 000 Bits pro Sekunde). Die durchschnittliche Netzgeschwindigkeit in der Schweiz betrug 2016 18 Mbit/s (Breitbandverbindungen) – 60 000 Mal schneller als 1977. Die heutigen Kabel- und Mobilnetzübertragungsraten übertreffen selbst den internen Datentransfer der ersten Personal Computer. Ohne diese Vernetzbarkeit der Computer wäre die Entwicklung des Internet of Things bis zum heutigen Internet of Everything nicht möglich gewesen. 1969 wurden mit ARPA, dem Vorläufer des Internet, die ersten vier Computer verbunden, aktuell dürften rund zehn Milliarden Geräte an Netzen hängen.

3.1.1.3 Technologische Entwicklung in Zahlen III: Die Preisentwicklung der Hardware

Ausschlaggebend für die wirtschaftliche Massenanwendung war schliesslich die Preisentwicklung: Die Rechenleistung, die man für einen Franken erhält, wird alle zehn Jahre verhundertfacht. Was vormals aufgrund der Kosten und der komplizierten Anwendung nur Expertinnen und Experten in ausgewählten Bereichen der Forschung und Wirtschaft vorbehalten war, ist heute für den kommerziellen massenhaften Einsatz bereit.

3.1.2 Künftige Entwicklung

Langfristige Prognosen, was für Auswirkungen der technologische Fortschritt auf Gesellschaft und Wirtschaft haben wird, sind selbst dann schwierig, wenn die technischen Grundlagen bekannt sind. Ein Beispiel dafür ist die Bedrohung der Privatsphäre durch das Sammeln von Daten. Bereits 2010 sagte Eric Schmidt, der langjährige CEO von Google, über die Zukunft der Privatsphäre: „We know where you are. We know where you've been. We can more or less know what you're thinking about”. Dennoch haben damals wohl nur wenige die Bedeutung dieser Aussage erfasst. Zurzeit bahnen sich in verschiedenen Gebieten Innovationen an, deren Tragweite enorm sein dürfte: neue Schnittstellen zwischen Mensch und Maschine, die Entwicklung des Quantencomputers und das Internet der Nanodinge (s. folgende Ziffern).

3.1.2.1 Schnittstelle Mensch-Maschine

Die Schnittstelle zwischen Mensch und Cyberraum steht an der Schwelle zu einem neuen revolutionären Entwicklungsschritt: In Steuerungsdaten umgeformte Gedanken (Brain-Computer-Interface) sind die letzte Stufe der perfekten effizienten Benutzerfreundlichkeit. Diese Vernetzung von allem wird auch den Menschen nicht mehr ausschliessen. Sie unterstützen z. B. bereits heute behinderte Menschen und könnten sehr bald nach Tastatur, Maus und Touchscreens die Benutzerschnittstelle Mensch-Maschine revolutionieren. Auch gibt es bereits seit längerer Zeit Systeme zur Stimulation von Nerven- oder Hirngewebe zu therapeutischen Zwecken, wie z.B. Cochlea- und Hirnstamm-Implantate zur Übertragung akustischer Information im Fall von Taubheit. Inwiefern sich diese Technologien für eine direkte Informationsvermittlung vom Computer zum Gehirn eignen, ist aber noch unklar.

Der nächste Schritt, die Anbindung (Schnittstelle) des Menschen an das Internet, steckt noch in den Kinderschuhen, macht aber grosse Fortschritte, weshalb einzelne Experten bereits den Begriff des „Internet of Everything" (IoE) geprägt haben. Die lang-

fristigen Risiken dieser Entwicklung sind nicht zu übersehen. Solche neuen Schnittstellen könnten eines Tages die Vertraulichkeit selbst nicht ausgesprochener oder verschriftlichter Gedanken gefährden: In Daten umgewandelt wären sie im Netz den gleichen Risiken wie alle anderen Daten ausgesetzt. Letztlich könnte die Technologie dazu führen, dass die Überzeugung, die Gedanken seien die letzte Bastion der informationellen Selbstbestimmung und Privatsphäre, ihrer Grundlage beraubt würde. Noch handelt es sich um ein rein theoretisches Risiko, aufgrund der technologischen Entwicklung aber ist dieses Szenario nicht auszuschliessen.

3.1.2.2 Quantencomputer

Zwischen den USA, China und Europa ist ein Wettlauf entbrannt, wer als erster einen voll funktionsfähigen Quantencomputer entwickeln kann. Im Unterschied zu einem herkömmlichen Computer können die Qubits eines Quantencomputers eine Vielzahl von Zwischenzuständen gleichzeitig abbilden (exponentiell viele), was zu einer enormen Leistungsfähigkeit führt. Es ist wahrscheinlich, dass in den nächsten Jahren Quantencomputer die leistungsstärksten konventionellen Computer hinter sich lassen – allerdings nur im Bereich spezifischer mathematischer Aufgabenstellungen.

Mit der weiteren Entwicklung der Quantencomputer werden die Applikationen auch für weitere Anwendungen u.a. im Bereich der Chemie interessant um z.B. die Reaktionen komplexer Moleküle zu modellieren, was heute mit Computern nicht möglich ist. In 10-15 Jahren dürfte schliesslich ein Quantencomputer zur Verfügung stehen, der vielfältig anwendbar ist und z.B. in der Lage sein wird, die heute weitverbreiteten asymmetrischen Verschlüsselungstechniken, insbesondere RSA, zu brechen. Experten gehen davon aus, dass die Chancen, dass ein solcher Quantencomputer der dritten Generation innerhalb der nächsten zehn Jahre zur Verfügung stehen wird, bei 50 Prozent liegen. Die Folgen wären tiefgreifend, da die gesamte Sicherheit im Netz genau auf diesen Prinzipien mathematischer Komplexität beruht, die sich mit Quantencomputern lösen lässt (s. auch Ziff. 4.4.1).

3.1.2.3 Das Internet der Nanodinge

Die Digitalisierung der Welt durch die Vermessung und Steuerung mittels Daten wird zukünftig in alle Bereiche vordringen und bisher digitalferne Bereiche der Lebens- und Wirtschaftswelt erfassen. Sie wird noch tiefer in die Dinge selbst und in die belebte Welt - Pflanzen, Tiere, Menschen - vordringen. Nanosensoren – eine Technologie, die heute noch in den Kinderschuhen steckt – werden diese Aufgabe übernehmen und das „Internet of Things" in ein "Internet der Nanodinge" verwandeln. Auch diese cyberphysischen Instrumente auf Nanoebene werden nicht nur Daten erfassen, sondern als Aktoren im Nanobereich auf die reale Welt einwirken, sei es im medizinischen Bereich, sei es bei der Qualitätskontrolle oder bei der Selbstreparatur von Dingen durch neue Materialinnovation. Ein weiteres Anwendungsbeispiel wäre der Einsatz von Kleinstsensoren, die am Anfang einer Lebensmittelproduktionskette bei Nutztieren und Pflanzen eingesetzt werden und flächendeckend den Qualitätszustand der daraus gewonnenen Lebensmittel prüfen und allenfalls Alarm auslösen.

3.1.3 Die Auswirkungen des technologischen Fortschritts

3.1.3.1 Vom Computer zum „Internet of Things“

Waren ursprünglich nur Computer miteinander verbunden, lassen sich heute dank Miniaturisierung und drahtloser Datenübertragung alle Gegenstände miteinander verbinden. Das Internet of Things (IoT) kann dabei vom „Kühlschrank“ über tragbare digitale Endgeräte bis hin zu Körpersensoren (sogenannte „Wearables“) oder Drohnen alles Mögliche umfassen. Eine entscheidende Rolle bei dieser Entwicklung spielen cyber-physische Systeme, in denen mechanisch/analog funktionierende Elemente mit digitalen Informationselementen verschmelzen, Daten erheben, verarbeiten und als Aktoren wieder auf die Umwelt einwirken.

Diese Gegenstände und Applikationen des IoT sind so weit intelligent, dass sie ihre Umwelt wahrnehmen, aufnehmen, vermessen und auch selbst angesteuert werden können. Ihre Intelligenz beschränkt sich aber auf die Datenerstellung bzw. die Umsetzung von datengesteuerten Befehlen. Das liegt daran, dass die Geräte, selbst ein Smartphone, weder über die nötige Rechenleistung verfügen noch die nötigen Datenmengen speichern können, wie sie zum Beispiel bei einer Sprachsteuerung nötig sind. So beziehen die Geräte Ihre eigentliche Intelligenz durch die Vernetzung mit einer zentralen cloudbasierten Datenbearbeitung.

Das IoT ist ein Hinweis darauf, was in Zukunft Realität sein wird. Prognosen gehen davon aus, dass in zwei Jahren 1 Milliarde PC, 5 Milliarden Smartphones und 25-30 Milliarden vernetzte Dinge Daten erheben und untereinander austauschen werden. 3,5 Milliarden Menschen benutzten 2016 das Internet. Im Mai 2018 waren erstmals mehr als die Hälfte der Erdbevölkerung im Internet, knapp 4 Milliarden Menschen.

Während IoT eher im Konsumenten- und Dienstleistungskontext benutzt wird, beschreibt „Industrie 4.0“ das gleiche Phänomen der Vernetzung im Bereich der Produktion. Wesentliches Merkmal der Industrie 4.0 ist die Anwendung datengestützter Kommunikation und Steuerung über den gesamten Organisations- und Produktionsprozess hinweg. Zum Beispiel kann so die Funktionalität von Produktionsstrassen in Echtzeit und höchst flexibel angepasst werden. Im Idealfall kommuniziert das Produkt während des gesamten Lebenszyklus‘ (Inbetriebnahme, Funktionskontrolle, Wartung, Funktionsausbau etc.) mit seiner Umgebung. Die Voraussetzung dafür ist: Die Maschinen müssen untereinander kommunizieren und sich im Idealfall selbst steuern können (M2M). Der ganze Wertschöpfungsprozess soll dabei „smart“ gestaltet werden. Dazu sind die Kontrolle und die Überwachung von Geräten und Prozessen über die Vernetzung mit der Informations- und Kommunikationsinfrastruktur zu verzahnen. Dies eröffnet u.a neue Möglichkeiten im Vertrieb: Die bisherigen Anbieter von Produkten können dazu übergehen, statt statischer Produkte auf die Kundenbedürfnisse zugeschnittene dynamische Servicedienstleistungen anzubieten. Noch ist dieser Ansatz für viele Wirtschaftssektoren ein Zukunftsprojekt.

Die intelligente Vernetzung cyber-physischer Systeme eignet sich auch dazu, grössere Systeme wie Verkehrsströme, Energieinfrastrukturen oder landesweite Logistikinfrastrukturen zu steuern. Sie kommen überall dort zum Einsatz, wo die systemische Kontrolle über vernetzte Steuerungsanlagen mit einer Vielzahl von Knotenpunkten immer komplexer wird und die Verarbeitung der Ausgangsdaten möglichst in Echtzeit zu geschehen hat. Auch hier steht die Entwicklung allerdings erst am Anfang.

Die Entwicklung des IoT in allen Lebensbereichen macht wie kaum anderswo deutlich, dass beim Zusammenspiel aller betroffenen Stakeholder der regulatorische Hand-

lungsbedarf geklärt werden muss. Das betrifft technische Normen oder Sicherheitsstandards, datenschutzrechtliche Aspekte, Fragen der Haftung, den Konsumentenschutz aber auch wettbewerbsrechtliche Fragen.

3.1.3.2 Cloud-Computing

Dank schneller Breitbandverbindungen brachte die Auslagerung der Datenspeicherung und Datenbearbeitung in die „Wolke“ (Cloud-Computing) die nötige Ressourcenflexibilität und Effizienz, Kostenersparnisse durch Skalierung sowie Spezialisierung, um mit den steigenden Datenmengen umgehen zu können. Bezüger von Cloud-Dienstleistungen können dank Cloud-Computing ihre spezifischen und variierenden Rechen- und Speicherkapazitäten nach Bedarf beziehen. 2017 hat die Anzahl cloudgestützter Server die Anzahl firmeneigener Server überholt. Auch die Welt der „Apps“ ist ohne Cloudinfrastruktur undenkbar, bei der sich die Nutzer weder um die Infrastruktur noch um die Plattform, die Anwendung oder die Daten kümmern müssen. Voraussetzung für das Cloud-Computing sind stabile, leistungsfähige und hochverfügbare fest- und mobilnetzgestützte Breitbandverbindungen.

Den Vorteilen des Cloud-Computing stehen auch Nachteile wie eine zunehmende Abhängigkeit vom Provider (lock-in-Effekte) und Sicherheitsbedenken gegenüber. Die Auslagerung von sensitiven Daten oder von Daten, deren Bearbeitung - wie etwa bei personenbezogenen Daten - gesetzlichen Bestimmungen unterworfen ist, stellt ein Risiko dar. So ist die Vertraulichkeit der Daten gefährdet, wenn der Cloud-Anbieter in einem Abhängigkeitsverhältnis zu einem fremden Rechtssystem steht oder aus anderen Gründen die Daten seiner Kunden fremden Behörden herausgeben muss. Oftmals weisen diese Rechtssysteme eine extraterritoriale Reichweite auf (s. auch Ziff. 8.2.7).

3.1.3.3 Siegeszug der unstrukturierten Daten: Big Data (Massendaten)

Daten können direkt durch menschliche Aktivitäten entstehen wie etwa bei Suchanfragen, bei geschäftlichen Transaktionen im Netz, sozialen Interaktionen auf den Plattformen oder einfach bei der Erstellung von Dokumenten, E-Mails oder SMS. Eine ungleich grössere Datenmenge wird bereits heute durch technische Systeme generiert wie etwa Steuerungs- und Kontrolldaten in der Produktion oder bei der Gebäudetechnik. Wesentlich ist die Vernetzung dieser Steuer- und Sensorgeräte über das Netz: Die erhobenen Messdaten müssen nicht wie früher durch den Menschen manuell in die digitalen Infrastrukturen eingegeben werden; sie werden automatisch überführt und gespeichert.

Durch die steigende Menge von Sensoren wird die reale Welt immer feinkörniger und flächendeckender vermessen, erfasst und in Echtzeit in Daten repräsentiert. Dazu gehören auch die Randdaten, die den Gebrauch elektronischer Geräte festhalten, wie etwa Mobiltelefone. Diesen Daten gehen in der Regel menschliche Aktivitäten voraus, womit sie zwar auf den ersten Blick Sachdaten sind, aber sehr viele indirekte Informationen über Personen beinhalten können. Damit wird die bisherige statische Unterscheidung zwischen Personen- und Sachdaten zunehmend vage, was vor allem im Bereich des Datenschutzes brisante Fragen aufwirft.

Folgende Faktoren treiben die Bedeutung von Daten weiter voran:

- Daten lassen sich heute in einem bis vor kurzem undenkbaren Ausmass und mit Grenzkosten nahe dem Nullwert kopieren, versenden, weiterverarbeiten, speichern und allen zur Verfügung stellen.

- Technologie und Wirtschaft stellen den IKT-Benutzern immer benutzerfreundlichere digitale (End-)Geräte zu immer tieferen Anschaffungskosten zur Verfügung. Der Zugang zum Cyberraum steht heute fast jedem offen. In den Erstweltländern dürften heute annähernd 100 Prozent aller Bewohner mit tragbaren internetfähigen Geräten einen beinahe permanenten Zugang zum digitalen Raum haben.

Die Daten als kleinste Informationseinheit sind zur Grundeinheit der digitalen Transformation geworden. Die Zunahme der Datenmenge ist beindruckend. Das Datenvolumen verdoppelt sich jedes Jahr, Tendenz steigend. Im Jahr 2020 dürfte die Menge erzeugter Daten 40 Zettabytes (10^{21}) überschreiten.[1] Täglich werden etwa 4000 Petabytes (1 Petabyte entspricht 10^{15} Bytes) über das Internet transportiert. Alle jemals in der Menschheitsgeschichte geschriebenen Texte entsprechen etwa 100 Petabytes. Schätzungen zufolge werden an einem beliebigen Tag 2018 rund 280 Milliarden E-Mails versandt und 3,5 Milliarden Suchanfragen via Google gestartet.[2]

Big Data (Massendaten) hat sich als Überbegriff für diese Datenflut eingebürgert. „Big Data“ beschreibt ein Phänomen, das sich definiert durch folgende Dimensionen: die Geschwindigkeit, mit der Daten gesammelt, generiert und transferiert werden (velocity), das Datenvolumen (volume), die Qualität und Glaubwürdigkeit der Daten (validity/veracity) und die Unterschiedlichkeit der Daten (variety). Variety bezieht sich auf die Vielfalt der Datentypen: Das können herkömmliche Datentypen, aber auch Bilder, Videos, Sprachaufzeichnungen oder E-Mails sein. Bei Big Data liegen heterogene Daten in unterschiedlichsten Datenformaten vor. Die Inhalte der Daten bei Big Data sind nicht strukturiert und lassen sich nicht in die Datenstruktur einer herkömmlichen relationalen Datenbank einfügen und bearbeiten.

Schätzungen gehen davon aus, dass weit über 90 % aller Daten in unstrukturierter Form vorliegen. Big Data Analysetools (Big Data Analysen, s. nachfolgende Ziff.) erlauben die Bearbeitung und Auswertung grosser Mengen an unstrukturierten Daten. Allerdings zeigt die Entwicklung, dass die Speicherung von Daten viel schneller voranschreitet als deren Auswertung. Neben den fehlenden kostengünstigen Analysetools und der Expertise ist die unterschiedliche Entwicklung der Rechengeschwindigkeit im Unterschied zur Speicherkapazität ein Erklärungsgrund dafür.

Gemeinhin werden Daten als das Öl des 21. Jh. bezeichnet. Trotz der Ökonomisierung der Daten lässt sich ihr Wert kaum fassen. Die Schätzungen/Berechnungen, was ein Datensatz über eine Person wert ist, gehen weit auseinander und sind nur indirekt eruierbar. Bei Google müsste der Wert bei einem Jahresumsatz von 80 Milliarden USD und knapp zwei Milliarden Nutzern ca. 40 USD pro Nutzer betragen. Anhaltspunkt für den Wert der Daten können auch Übernahmen von Unternehmen sein, die mit Daten arbeiten. Facebook hat 2014 für WhatsApp mit damals 600 Mio. Nutzern 19 Milliarden bezahlt, was einen Wert von 32 USD pro Nutzer ergibt. IBM bezahlte pro Nutzer rund 12 USD bei der Übernahme von Truven Health Analytics, Microsoft hingegen 58 USD für den Kauf von LinkedIn. So unsicher die Zahlen auch sind, so zeigen sie deutlich,

[1] Data Age 2015. The Evolution of Data to Life-Critical: https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf [Stand 7.6.2018]

[2] http://www.internetlivestats.com [Stand April 2018]; The Radicati Group, Inc. Email Statistic Report, 2017-2021. 2017. https://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf.

dass Unternehmen bereit sind, hohe Summen für personenbezogene Daten zu investieren.

3.1.3.4 Big Data Analysen (Big Data Analytics)

Technisch gesehen ermöglichen die Big Data Analysen die Auswertung grosser unstrukturierter Datenmengen. Der Big Data Ansatz überprüft häufig nicht Thesen anhand erhobener Daten, sondern erkennt mittels statistischer Analyse von Massendaten Korrelationen und Wechselwirkungen, die auf Verhaltens- und Ereignismuster hinweisen. Dies kann sogar in Echtzeit erfolgen. Die gewonnenen Ergebnisse sollen dabei helfen, Produktions-, Betriebs-, Vertriebs- und Verwaltungsprozesse aller Art zu verbessern, Risiken zu reduzieren, beim Eintretensfall schneller zu reagieren, Verhaltensweisen und Ereignisse besser voraussehen zu können und entsprechend zu handeln. Das enorme Entwicklungspotenzial liegt auf der Hand – für die Wirtschaft, die Verwaltung und das Gemeinwohl.

Die Daten werden dabei zu einer neuen Quelle der Wertschöpfung, indem sie Erkenntnisse ermöglichen, für die sie z.T. ursprünglich gar nicht aufgenommen worden sind. Aus diesem Grund spricht man auch von einer Wiederverwertung von Daten (Data Recycling). Big Data Analysen verändern damit den bisher statischen Lebenszyklus von Daten in strukturierter Form. In Einzeldaten aufgebrochene Datensätze können durch Korrelationen entweder völlig neu zusammengesetzt oder zu ihrer ursprünglichen Datendichte im Datensatz zusammengefügt werden. Dies hat Auswirkungen auf die Bearbeitung von personenbezogenen Daten, die Möglichkeiten und Grenzen der Anonymisierung und damit auf den Datenschutz (s. Ziff. 5.3.1.6).

Wie bei jeder Technologie liegen die Chancen wie ein verbessertes Risikomanagement oder eine optimierte Funktionalität und die Risiken wie die Vorhersehbarkeit des menschlichen Handelns und damit die Möglichkeit zur Diskriminierung und Manipulation eng beieinander. Beispielsweise wird beim oft genannten „predictive Policing“ anhand der Mustererkennung vergangener Straftaten der Ressourceneinsatz der Polizeikräfte gesteuert. Dies könnte dazu führen, dass jemand präventiv verdächtigt wird, weil er morgen gemäss Big Data Analysen ein Verbrechen begehen könnte.

Grundlegende Herausforderungen stellen sich aber nicht nur bei personenbezogenen Daten. In der Produktion und bei Organisationsprozessen stehen heute Massendaten zur Verfügung. Die Produktionsinfrastrukturen messen zwar die Daten und halten sie fest, aufgrund fehlender Analysetools und der nötigen Expertisen findet aber eine konstruktive Auswertung nur unzureichend oder gar nicht statt.

Im Zusammenhang mit Big Data Analysen sind vor allem zwei Risiken zu beachten:

- Die analytische Methode und die breite Datenbasis bei Big Data Analysen verleiten dazu, die Ergebnisse als objektiv einzustufen. Das wäre falsch: Big Data Analysen liefern nicht rationale Entscheidungsgrundlagen, sondern stellen lediglich ein auf Wahrscheinlichkeitsrechnungen basiertes Hilfsinstrument für eine bessere Entscheidungsfindung zur Verfügung.
- Big Data Analysen beruhen auf Algorithmen und z.T. auch auf selbstlernenden Algorithmen, deren Anwendung ein beträchtliches Fehlerpotenzial aufweist.

3.1.4 Algorithmen

3.1.4.1 Einführung

Algorithmen sind für den Computer Schritt-für-Schritt-Handlungsanweisungen (Programme), mit denen eine Aufgabenstellung gelöst werden kann. Algorithmen bestehen aus endlich vielen, klar definierten Abarbeitungsschritten, die meist aus einer höheren, für den Menschen einfacher zu begreifenden Programmiersprache (Quellcode) durch ein Übersetzungsprogramm (Compiler) in für die Computerhardware verarbeitbare Einzelinstruktionen (Maschinensprache) übersetzt werden. Abhängig von den zu verarbeitenden Daten werden in den Algorithmen unterschiedliche Pfade in vorgegebenen Entscheidungsbäumen durchlaufen. Bei traditionellen deterministischen Algorithmen führen dieselben Eingaben auch immer zu denselben Ausgaben oder Entscheidungen, da die Entscheidungsprozesse sich nicht ändern.

Die Künstliche Intelligenz (KI) bedient sich häufig sogenannter selbstlernender Algorithmen, die mit Daten trainiert werden und deren Ablauf nicht mehr deterministisch ist, sondern davon abhängt, mit welchen Daten sie trainiert wurden. Das heisst aber nicht, dass sich die Algorithmen selbst verändern, sondern dass sie selbstständig ihre Entscheidungsprozesse modifizieren. Diese Algorithmen selbst müssen initial immer noch programmiert werden und kommen z.B. als sogenannte deep Neural Networks (DNN) zum Einsatz. DNN können dann für Bild- oder Spracherkennung eingesetzt werden. Dies ist eine neue Qualität von Algorithmen, da je nach verwendeten Trainingsdaten in der Lernphase der Algorithmus im produktiven Einsatz bei denselben Eingabedaten zu unterschiedlichen Ausgaben oder Entscheidungen kommen kann.

3.1.4.2 Künstliche Intelligenz (KI)

Voraussetzung für den technologischen Durchbruch waren die massive Steigerung der Rechenleistung in den vergangenen 15 Jahren und die relativ einfache Verfügbarkeit von vielen Trainingsdaten für die Anwendung selbstlernender Algorithmen.

Noch 2015 glaubte man, es würde noch mindestens fünf Jahre dauern, bis ein Computer die weltbesten Spieler im Brettspiel Go schlagen könne. Doch bereits im März 2016 schlug AlphaGo von Google den Weltmeister in vier von fünf Spielen. Dies dürfte ein weiterer Schritt in die Richtung sein, an deren Ende selbstdenkende Systeme stehen.

Der Anwendungsvielfalt sind keine Grenzen gesetzt: KI kann ermüdungsfrei, schnell, kostensparend und in immer gleicher Qualität anspruchsvolle Aufgaben übernehmen. Die Delegation an die Maschine bietet sich auch dort an, wo die Maschine wie etwa bei Kontroll- und Überprüfungsarbeiten unter Ausschluss einer natürlichen Person mehr Anonymität in Aussicht stellt. So erstaunt es nicht, dass die Wirtschaft massiv investiert.

3.1.4.3 Herausforderungen durch Algorithmen

Algorithmen sind das Fundament der Datenbearbeitung. Da die neuen Algorithmen im Bereich von Big Data Analysen und vor allem der KI noch Gegenstand intensiver Forschung sind, ist auch den Risiken besonders Rechnung zu tragen.

Die Verfügbarkeit und die Qualität des Datenmaterials sind bei selbstlernenden Algorithmen bedeutsam: Das Datenmaterial kann falsch, unvollständig, veraltet oder nicht feinkörnig genug sein. Insbesondere Deep Learning Systeme sind anfällig für historisch gewachsene Vorurteile, die ihren Niederschlag im Trainingsmaterial (z.B. Daten

aus dem Netz) für die Algorithmen gefunden haben. Bekannt wurden zwei Pannen bei Google und Flickr, als deren Gesichtserkennungssysteme Menschen schwarzer Hautfarbe als Gorillas einordneten. So können sich Vorurteile durch die Hintertür einer vermeintlich objektiven Datenbearbeitung in ein objektives Faktum verwandeln und die Entscheidungsfindung massgeblich beeinflussen. Die Verwendung von z.T. unkontrollierten Massendaten einer digitalisierten Gesellschaft führt dazu, dass selbstlernende Algorithmen das wiedergeben, was sie von dieser Gesellschaft gelernt haben.

Fehler können sich bei der Konstruktion des Entscheidungssystems und bei dessen Evaluation einschleichen. Auch korrekte Algorithmen, eine adäquate Operationalisierung und die richtige Datenmenge und -qualität können fehleranfällige Entscheidungsprozesse nicht verhindern, bei denen die Gewichtung der einzelnen Messdaten und falsche Rückkoppelungen zu falschen oder verzerrten Resultaten führen. Schliesslich wird die Entwicklung selbstlernender Systeme die Anwender herausfordern, die ständig sich anpassende Funktionsweise (wechselnde Variablen und Gewichtung) ihrer intelligenten Maschinen nachzuvollziehen. Bereits der heutige Stand der Technik führt zu Situationen, in denen die Betreiber den Lösungsweg eines Deep Learning Systems nicht mehr nachvollziehen können.

Die Erarbeitung von Entscheidungsprozessen mit Algorithmen bedingt eine hochgradig interdisziplinäre Zusammenarbeit von Datenanalysten, Programmierern, Algorithmusspezialisten und je nach Fragestellung spezifischen Sektor-Experten (aus Politik, Werbung, Psychologie, Soziologie, Kommunikation, Produktionsanlagen, etc.). Diese Zusammenarbeit setzt ein übergreifendes Fachwissen und ein gemeinsames Verständnis voraus, was selten gegeben ist.

Die Bedeutung insbesondere selbstlernender Algorithmen wird zunehmen und Auswirkungen auf die Gesellschaft haben. Bei der Datenbearbeitung von Gemeinschaften sowie juristischer und insbesondere natürlicher Personen kann es zu fehlender Fairness und zu systemischer Diskriminierung bis hin zur Verletzung rechtlicher Bestimmungen kommen.

3.1.4.4 Risikominimierung bei Algorithmen

Massnahmen zur Risikominimierung bei Algorithmen sind auf drei Ebenen möglich: auf der rechtlichen Ebene, auf der Ebene der guten Praxis und im Bereich ethischer Überlegungen.

Algorithmen im Rahmen gesetzlicher Regelungen
Die beginnende Diskussion thematisiert die Herausforderungen der Algorithmen vor allem im Kontext des Datenschutzes. Bei der Arbeit mit Algorithmen sind ohne Zweifel die Prinzipien der Transparenz und der Zweckbindung einzuhalten. Die Beachtung dieser Prinzipien kann sich indessen nicht allein auf die Dateneingabe und -ausgabe von Algorithmen beschränken, weil ein Anwender von Algorithmen in selbstlernenden System die sich abspielenden Entscheidungsprozesse nicht nachvollziehen kann, was den beiden Prinzipien widerspricht.

Zudem kann ein verantwortlicher Datenbearbeiter bei dieser Ausgangslage keine Risikofolgenabschätzung aus datenschutztechnischer Sicht mehr erstellen, wie sie in der Datenschutz-Grundverordnung der EU vom 27. April 2016 (DSGVO) bzw. in der Botschaft E-DSG vorgesehen ist. Der Datenschutz hält zwar fest, was ein Algorithmus bei der Datenbearbeitung zu leisten hat bzw. leisten darf, er ist aber nicht dafür ausgerichtet, auf einer technischeren Ebene das „Wie“ im Detail zu definieren. Allerdings wurden bei der Weiterentwicklung des Datenschutzes bei der DSGVO und beim E-DSG neue

technische Regelungen wie „Privacy by Design“ (Datenschutz durch datenschutzfreundliche Technikgestaltung) berücksichtigt. Abgesehen von generischen Grundsätzen – wie Datenminimierung, Pseudonymisierung und Anonymisierung sowie Datensicherheit gemäss Stand der Technik – sind die Prinzipien der Privacy by Design nicht im Detail ausgeführt und bereits seit längerer Zeit Bestandteil einer intensiven Diskussion. Welche detaillierten technischen Anforderungen schliesslich nur den Stand der guten Praxis wiedergeben oder bereits einen de facto Standard mit Blick auf die rechtliche Ausgestaltung definieren sollen, ist noch nicht geklärt. Im Fokus dieser Diskussionen standen aber nie die Algorithmen selber als Basis der modernen Datenbearbeitung, sondern generelle Betrachtungen über eine datenschutzfreundliche Technikgestaltung bzw. die Herausforderungen durch Big Data Analysen.

Spezifische datenschutztechnische Probleme ergeben sich beim Prinzip der Transparenz von Algorithmen, da diese Geschäftsgeheimnisse enthalten können und als Geschäftsinvestition zu schützen sind. So muss der Datenbearbeiter bei automatisierten Einzelentscheiden die Grundannahmen des Algorithmus offenlegen, nicht aber die Algorithmen selbst oder die Grundstruktur der Entscheidungsprozesse (Art. 23 Abs. 2 lit. f E-DSG). Eine Konkretisierung, wie weit eine Offenlegung zu gehen hat, gibt es noch nicht. Zwei Ansätze sind denkbar:

Bei einer weitmaschigen Auslegung der Offenlegungspflicht zugunsten der Datenbearbeiter müssten nur die Grundannahmen genannt werden, die beim Beschrieb des algorithmischen Systems einen Bezug zu den massgeblichen Grundsätzen und gesetzlichen Regelungen in einem spezifischen Einsatzgebiet aufweisen. Als spezifische gesetzlich geregelte Bereiche sind etwa das Gesundheitswesen, der Konsumentenschutz oder das Steuerrecht zu nennen.

Bei einer restriktiveren Auslegung gemäss der Working Group 29 der EU zum Datenschutz[3] müssten die Grundannahmen, aber auch der Weg (in diesem Fall der Entscheidungsprozess), die Schlüsselfaktoren für die Entscheidungsfindung und deren Gewichtung offengelegt werden. Dies steht aber im Widerspruch zum Grund Nr. 63 in der DSGVO, der die Rechte und Freiheiten anderer Personen wie etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums priorisiert. Es ist zu erwarten, dass Praxis, Rechtsprechung und Leitlinien der Aufsichtsbehörden mehr Klarheit bringen werden. Dies wird allerdings dadurch erschwert, dass der technologische Fortschritt bei den Algorithmen die Möglichkeit der Aufwertung einzelner Sachverhalte zu Präzedenzfällen mit allgemeiner Aussagekraft für gleich gelagerte Fälle verringern wird.

Die Herausforderungen durch Algorithmen wären neuerdings auch im Rahmen des Kartellgesetzes diskutiert. Algorithmen vermögen zu einem wettbewerbswidrigen "abgestimmten Verhalten" im Sinne einer horizontalen Absprache zwischen Konkurrenten zu führen, sofern sie sich gleichmässig verhalten. Gesprochen wird dabei von einer sogenannten "Kollusion" (s. Ziff. 6.3.3).

Massnahmen der guten Praxis und ethische Aspekte

Massnahmen der guten Praxis beim Entwurf der Algorithmen, die sich die Anwender selbst auferlegen, könnten ebenfalls zu mehr Sicherheit und Vertrauen führen. Zu den Massnahmen guter Praxis könnte gehören, dass Entwickler und Anwender:

- Grundannahmen, Funktionsweise der Algorithmen und Entscheidungsprozesse offenlegen;

[3] Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

- bei der Implementierung und Evaluation selbstlernender Systeme verstärkt die Resultate plausibilisieren;
- im Sinne einer verbesserten Risikosensibilisierung die Nutzer über die möglichen negativen Folgen ihrer algorithmischen Datenbearbeitung informieren;
- bei den Trainingsdaten auf Korrektheit, Vollständigkeit und auf den Zweck zugeschnittenen maximal aggregierten Zustand von Daten achten;
- in der Grundstruktur der selbstlernenden Maschine ein automatisiertes Prüfprogramm implementieren;
- insbesondere rekursive, sich selbst verbessernde Systeme einer verstärkten Kontrolle durch Dritte unterstellen.

Selbstlernende Algorithmen machen ein technik-, rechts- und fairnessbedingtes System nötig, das fortlaufend nichtbeabsichtigte, rechtswidrige und „unfaire“ Behandlung von Nutzern aufgrund entsprechender Muster transparent macht und natürliche Personen bei der Kontrolle unterstützt. Dieses System müsste bereits bei der Dateneingabe ansetzen und zwischen sensitiven (Rasse, Geschlecht), kontextbezogenen und sonst differenzierenden Attributen (notwendig, nützlich bis diskriminierend) unterscheiden und deren Anwendung im Entscheidungsprozess erkennen. Schliesslich muss die Verknüpfungsqualität zwischen dem Ergebnis des Entscheidungsprozesse und der Attribute statistisch untersucht werden. Die Ergebnisse liefern die Grundlage, um die Funktionsweise des Algorithmus nachzuvollziehen und systemische negative Auswirkungen auf Nutzergruppen zu identifizieren. Die Entwicklung solcher Testprogramme ist zurzeit Gegenstand der Forschung, die aber weiter intensiviert werden muss, damit möglichst rasch marktfähige Systeme zur Verfügung stehen.

Weitere technische und organisatorische Massnahmen wären zu erarbeiten und zu prüfen. Schliesslich könnten für die Entwicklung von Algorithmen ethische Prinzipien aufgestellt, allenfalls auch eine Berufsethik für Datenanalysen entwickelt werden. Ein Element dieser Ethik für Algorithmen wäre u.a. die Kompatibilität mit den Idealen kultureller Vielfalt, Freiheit, Menschenrechten und Würde (s. auch Ziff. 11).

3.2 Pull-Faktoren

3.2.1 Wirtschaft

Zentraler Pull-Faktor für die digitale Transformation ist die Wirtschaft, die neue Geschäftsmodelle, insbesondere internetunterstützte Dienst- und Informationsleistungen, eine verbessertes Risikomanagement und bessere Entscheidungsgrundlagen entwickelt. Die Digitalisierung verspricht neue Chancen, sich Konkurrenzvorteile zu erarbeiten: Automatisation sowie optimierte und flexible Produktionsketten führen zu Effizienz- und Produktionssteigerung. Bahnbrechend ist die Möglichkeit der individualisierten Massenanfertigung von Gütern und von Dienstleistungen. Voraussetzung dazu ist die neue Nähe zum Kunden über digitale Vertriebswege und Plattformen sowie ein ausgeklügeltes Kundenprofiling, das den Massenkunden in einen Einzelkunden verwandelt und damit auch die Kundenbindung verbessert. Im B2C-Bereich stehen wir bereits mitten in dieser Entwicklung; im B2B-Bereich dürfte die Tendenz verstärkt auch in diese Richtung gehen.

Die Digitalisierung der Prozesse zwischen Kundinnen und Kunden bzw. Anbietern einerseits und Anbietern und deren Lieferanten andererseits erlaubt es, bestehende

Wertschöpfungsketten neu zu definieren und Intermediäre auszuschalten. Dabei besteht ein entscheidender Pull-Faktor darin, im vorgelagerten Bereich zum Kunden hin Daten zu sammeln. Die Auswertung der Daten und der Einsatz digitaler Kommunikationsmittel haben zum Ziel, den Vertrieb zu optimieren und das Geschäftsmodell so weiterzuentwickeln, dass anstelle von Produkten und Gütern ganzheitliche Dienstleistungen angeboten werden können.

Im Bereich Betrieb bietet die Digitalisierung neue Möglichkeiten: Sensortechnik, Datenerfassung und -auswertung ermöglichen eine verbesserte Systemüberwachung in Echtzeit und ein entsprechendes anspruchsvolles Qualitätsmanagement – im Idealfall über den ganzen Lebenszyklus des Produkts hinweg und unter Berücksichtigung ausgebauter Support- und Wartungsleistungen beim Kunden. Mit den gewonnenen Daten lassen sich operative und geschäftliche Risiken reduzieren und bessere Entscheidungsgrundlagen bereitstellen.

3.2.2 Forschung

Nicht nur die Wirtschaft, sondern auch die Forschung ist eine der treibenden Kräfte der digitalen Transformation und Datifizierung. Hauptsächlich geht es in der Forschung um neue Forschungsmethoden, die dank der Menge, Feinkörnigkeit, Verfügbarkeit, globalen Herkunft, Aktualität und Analysierbarkeit der Daten möglich werden.

3.2.3 Konsumenten und Nutzer digitaler Dienste und Plattformen

Konsumentinnen und Konsumenten sowie Nutzerinnen und Nutzer spielen eine entscheidende Rolle als Pull-Faktor: Digitale Dienste und Plattformen bieten ihnen einen unlimitierten, ortsunabhängigen und permanenten Zugang zu Informationen, Dienstleistungen, Gütern, Unterhaltungsmöglichkeiten und sozialen Online-Netzwerken. Universale Plattformen vereinen inzwischen verschiedenste Dienstleistungen wie Informationssuche, „Shopping“ und virtuelle Begegnungs- und Ausstellungsräume.

Konsumenten und Nutzer haben sich daran gewöhnt, dass vielerlei Dienste, Informationen und Produkte im Rahmen des Freemium-Geschäftsmodells „gratis“ sind. Dies führt wiederum zur datenschutztechnischen Frage, ob die Preisgabe der Privatsphäre und der informationellen Selbstbestimmung grundsätzlich gegen die gesetzlichen Rahmenbedingungen verstösst oder mit entsprechenden Auflagen als Entgelt akzeptiert werden sollte (s. Ziff. 7.2.4). Eine solche Monetarisierung personenbezogener Daten wird alle Teilnehmer dieses wirtschaftlichen Netzwerkes mit der Frage konfrontieren, wie der Austausch zwischen Privatsphäre und Dienstleistung zu gestalten ist.

Konsumenten und Nutzer haben die Breite, die Qualität und vor allem den Komfort all dieser Leistungen und integraler Ökosysteme als einen nicht mehr wegzudenkenden Bestandteil ihrer Lebenswelt internalisiert. Die digitalen Dienstleistungen bieten ihnen niedrige Transaktionskosten, Zeitersparnis und zeitliche Unabhängigkeit, ohne die sie ihren Alltag nicht mehr meistern möchten. In vielen Bereichen kann und will der Konsument die frühere Wissensasymmetrie gegenüber dem Anbieter nicht mehr akzeptieren. Auf Knopfdruck kann er global Preise, Dienstleistungen, Konsumgüterqualitäten vergleichen und preislich von einer globalen Konkurrenzsituation profitieren. Die Teilhabe an sozialen Online-Netzwerken ist für viele eine Selbstverständlichkeit geworden und hat längst eine kulturprägende Bedeutung erlangt.

3.2.4 Der Staat

Die militärische Forschung hatte wesentlichen Anteil bei der Entwicklung der Rechenkapazität und der ersten Computer-Netzwerke. Sie spielt immer noch eine bedeutende Rolle, insbesondere im Bereich der Informationssicherheit und als Inkubator für die Grundlagenforschung wie etwa in der Robotik. Der militärisch-industrielle Komplex hat aber als technologischer Taktgeber bei der Datenverarbeitung an Bedeutung verloren.

Auf der Anwenderseite hingegen nimmt die Bedeutung des Staates als Treiber der digitalen Transformation zu, indem er E-Government konsequent und flächendeckend anbietet und die dafür notwendigen Infrastrukturen wie Breitbandanschluss, Mobilnetze oder die Möglichkeit zur elektronischen Signatur zur Verfügung stellt. Es ist aber auch nicht zu übersehen, dass die digitalen Infrastrukturen dem Staat neue Möglichkeiten der datengestützten Überwachung und sogar sozialen Disziplinierung und Sanktionierung ermöglichen, deren Kontrolle in entsprechender Weise durch die rechtsstaatlichen Instanzen sichergestellt werden muss. Schliesslich sammelt der Staat grosse Mengen an Daten, was ihn neben den Techgiganten und grossen Datenbrokern zu einem der grössten Datenbearbeiter macht und die Forderung nach einem entsprechenden Datenschutz und Open Government Data (OGD) erklärt.

4 Analysefeld Informationssicherheit

4.1 Ist-Zustand und die weitere Entwicklung

Statistiken über den Zustand der Sicherheit bei den digitalen Infrastrukturen im Allgemeinen und das Ökosystem Internet („Internet Interconnection Ecosystem"[4]) im Besonderen ist mit Vorsicht zu begegnen. Die Zahlen zeigen aber, welche Grössenordnungen hier im Spiel sind und in welche Richtung die Entwicklung geht: An einem beliebigen Tag 2017 wurden bis zu 65 000 Internetseiten gehackt, Analysesysteme erfassten alle 4,2 Sekunden eine neue Malware-Signatur. Die Anzahl unbekannter Schwachstellen, die im Netz herumgereicht werden, und für die es noch keine Korrekturen gibt, steigt (sogenannte Zero-Day-Exploits).[5] Im Jahr 2017 hat die Zahl entdeckter Software-Schwachstellen und deren Schweregrad einen Höchststand erreicht, insbesondere die Schwachstellen auf Prozessorebene steigen funktional an. Waren es noch vor ein paar Jahren ein paar wenige, ist deren Anzahl heute bereits im höheren zweistelligen Bereich. Verwundbarkeiten auf Chipebene, wie anfangs Jahr publiziert (Meltdown, Spectre), bedeuten nicht weniger, als dass das Betriebsprogramm und die darauf laufenden Applikationen der Basisinfrastruktur des Computers, dem Chip, nicht mehr vertrauen dürfen. Dies zeigt eine völlig neue Qualität der Bedrohung auf. Es ist zu befürchten, dass es nur eine Frage der Zeit ist, bis die ersten Cyberangriffe erwiesenermassen auf solche Schwachstellen zurückgeführt werden können.

2017 dürfte die Cyberkriminalität zum ersten Mal mehr Geld umgesetzt haben als das Drogengeschäft – die Schätzungen gehen von über einer halben Billion Dollar aus. Grössere Unternehmen wie Banken und die Verwaltung registrieren jeden Tag eine vierstellige Zahl von Angriffsversuchen. 90 % des Internets ist mit den gängigen Suchmaschinen nicht zu erreichen und entzieht sich als sogenanntes Deepnet oder Darknet (u.a. via Tor, Freenet oder I2P) der Möglichkeit der strukturierten Suche. Dies lässt sich kaum überwachen; böswillige Akteure mit entsprechendem Wissen und Zugangsmöglichkeiten können sich unbehelligt von Recht und Ordnung darin bewegen.

Auch mehren sich die Ausfälle von digitalen Dienstleistungen aufgrund von Fehlmanipulationen, Soft- oder Hardwareproblemen. Die Erwartungen an einen unterbruchsfreien Betrieb der digitalen Infrastrukturen sind höher als ihnen die Betreiber entsprechen könnten. Zunehmende Komplexität und Vernetzung der Systeme sind die Ursache dafür.

Nur langsam setzt sich die Einsicht durch, dass der Einsatz digitaler Infrastrukturen nicht nur mehr Effizienz, Komfort und Funktionalität mit sich bringt, sondern angesichts der Sicherheits- und Stabilitätsanforderungen auch Kosten. Die Enden des Spannungsdreiecks Sicherheit/Funktionsstabilität, Komfort und Funktionalität gehen immer weiter auseinander, sowohl bei Unternehmen als auch bei privaten Nutzern. Dies hat massive Folgen für die Datenbearbeitung, die untrennbar mit den digitalen Infrastrukturen verknüpft ist.

Es gibt aber auch positive Tendenzen: Die tägliche Berichterstattung über Datenverluste, Pannen und Dienstleistungsunterbrüche hat zu einem neuen Bewusstsein für IKT- und Informationssicherheit geführt. Das Thema ist mittlerweile allgegenwärtig. Über weite Strecken herrscht Einigkeit darüber, dass Handlungsbedarf herrscht. Mehrkosten für die IKT-Sicherheit werden nicht mehr nur als Kosten gesehen, die man sich

[4] Begriff nach ENISA (Europäische Agentur für Netz- und Informationssicherheit).

[5] http://www.internetlivestats.com/ [Stand Dezember 2017].

als vermeintlich tragbares Restrisiko wegwünscht, sondern als notwendige Investitionen. Die Einsicht hat sich durchgesetzt, dass eine digitale Transformation ohne Sicherheit und Vertrauen in die Informationssicherheit nicht nachhaltig sein kann.

4.2 Risiken im Bereich Informationssicherheit: Gefahren und Bedrohungen

Verschiedene Faktoren sind die Treiber für das Risiko Informationssicherheit. Dazu gehören die Entwicklung der Angriffsfläche, das wachsende Schadenpotenzial und die zunehmenden Gefahren und Bedrohungen. Dabei ist es wichtig, zwischen den vorsätzlichen Cyberangriffen (Bedrohungen) und den durch Fehlverhalten verursachten IKT-Zwischenfällen (Gefahren) zu unterscheiden.

4.2.1 Gefahren

4.2.1.1 Ökosystem Internet

Die Gründerväter des Internets suchten in den 1970er- und 1980er-Jahren nach einer technischen Lösung, um Computer möglichst effizient und einfach zu verbinden. Die Kernelemente waren ein dezentrales Netzwerk und Transportprotokolle, die alle Datenpakete ohne eine zentrale Koordinationsstelle von jedem Punkt des Netzwerkes zu einem anderen versenden konnten. In seiner Grundstruktur ist das Internet auf Offenheit ohne Schranken und Kontrollen sowie Verfügbarkeit ausgelegt. Jeder kann teilnehmen. 30 Jahre später sind diese Grundlagen immer noch das Rückgrat des Erfolgs des Internet, aber gleichzeitig auch dessen grösste Verwundbarkeit: Der Datenfluss ist nicht kontrollierbar, die Sicherheit der Daten gefährdet und die verschiedenen Akteure (Entitäten wie natürliche oder juristische Personen und technische Infrastrukturen) sind aufgrund der räumlichen Distanz nur mit einigem Aufwand authentifizierbar.

Viele Staaten haben reagiert und erlassen zunehmend Gesetze, die den freien Fluss der Daten im Internet blockieren, sei es zum Schutz der Privatsphäre, für eine bessere Kontrolle der Inhalte (z.B. das deutsche Netzwerkdurchsuchungsgesetz), aus Sicherheitsgründen, zwecks Zensur oder aus markttechnischen Überlegungen. Ein Mehrwert an digitaler Sicherheit zeichnet sich dadurch nicht ab, dafür aber die Gefahr, dass das Internet in einzelne Inseln zerbricht und die Qualität verliert, die es so erfolgreich gemacht hat. Vor diesem Hintergrund stellt sich die Frage, wie das Ökosystem Internet sicherer gemacht werden kann, ohne es zu zerstören (s. Ziff. 4.4.3).

4.2.1.2 Kein Allheilmittel gegen Cyberrisiken

Einzelne Schutzmassnahmen wie Firewalls oder Perimeterschutz genügen heute nicht mehr als Mittel gegen Cyberrisiken, wenn sie nur weit genug entwickelt und konsequent umgesetzt würden. Aufgrund des immer breiteren Waffenarsenals („blended Threats") und der Beharrlichkeit der Angreifer erweist sich dies als Irrglaube.

Die Notwendigkeit eines „Defense in Depth"-Ansatzes wurde lange nicht erkannt, der mehrere Verteidigungsebenen vorsieht, nicht erkannt. Hierzu müssen verschiedenste Verteidigungsmittel technischer Art („Firewall", „Anti Virus", Vulnerabilities Scanner") hintereinander gestaffelt und mit organisatorischen Massnahmen kombiniert werden. In einem komplexen System bietet sich auch die Anwendung gleicher Verteidigungstypen verschiedener Hersteller an. Trotzdem muss davon ausgegangen werden, dass

der Angreifer irgendwann einmal Erfolg haben wird. So gesehen sind nicht nur präventive Schutzelemente, welche die Eintretenswahrscheinlichkeit reduzieren, sondern auch reaktive Massnahmen wichtig, so die Fähigkeit, den Angriff zu erkennen und das System wiederherzustellen („Detection, Recovery").

Daher wird der Faktor Resilienz immer wichtiger: Die Fähigkeit, im Ereignisfall die Informationsverarbeitung auf einem minimalen Level weiterzuführen und den Datenverlust zu minimieren.

4.2.1.3 Komplexität durch Quantität und Vernetzung der digitalen Infrastrukturen und Daten

Als Folge der digitalen Transformation bauen die Organisationen immer mehr digitale Infrastrukturen, die sie vernetzen, damit komplexe und vielschichtige Verarbeitungsprozesse ohne Medienbrüche abgewickelt und Daten gemeinsam genutzt werden können. Der schnelle Aufbau erschwert es, die Übersicht über Prozesse, Systeme, Schnittstellen und Datenvolumen zu behalten. Bei Unternehmen fallen immer grössere und unstrukturiertere Datenmengen an, von denen sie nur einen Bruchteil auswerten und strukturiert ablegen können („dark Data"). So steigt auch das Risiko, nicht mehr zu wissen, wo und welche Prozesse und Daten sensitiv sind und entsprechend geschützt werden müssen. Oftmals reicht zudem eine Risikobetrachtung der Einzeldaten nicht aus, da gewisse Daten erst in ihrer Kombination oder durch die Menge sensitiv werden (Pooling-Effekt).

Die Prioritätensetzung fällt daher immer schwerer mit dem Ergebnis, dass die Organisationen alles schützen sollten. Weil es keine kostengünstigen Lösungen gibt und die Ressourcen für die Informationssicherheit oftmals fehlen, nehmen Verwundbarkeit und Risiko zu. Die aufgezeigte Tendenz zeigt sich aktuell bei der Umsetzung der DSGVO. Die Unternehmen müssen wissen, wo sie welche Daten gespeichert haben, was eine Grundvoraussetzung dafür ist, um die nötige Compliance überhaupt an die Hand nehmen zu können.

4.2.1.4 Fehlende Industrialisierung der Sicherheitssysteme

In den letzten 20 Jahren hat die Entwicklung der digitalen Infrastrukturen (vom einzelnen Computer bis zu komplexen digitalen Infrastrukturen) eine bemerkenswerte Industrialisierung durchlaufen. Ähnlich wie in der industriellen Fertigung, z.B. bei Autos, haben Standardisierung und Automatisierung die Funktionalität, die Kommoditisierung, die Auslagerung in die Cloud und die Benutzerfreundlichkeit massiv verbessert und eine kostengünstige Anschaffung ermöglicht. Davon hat auch die Sicherheit im Sinne einer „Security by Design" profitiert, dies aber nur bei einzelnen Komponenten und Dienstleistungen. Bei der Vernetzung der Systeme zu digitalen Infrastrukturen bietet die Industrialisierung noch keine standardisierten Sicherheitslösungen an. Fragmentierte Sicherheitssysteme aus Einzelkomponenten sind nicht integral aufgebaut, gefährden die Stabilität der Systeme und bieten keinen ganzheitlich durchdachten Schutz. Händisch erstellte spezifische Sicherheitslösungen sind zwar möglich, aber ressourcen- und kostenintensiv, da dafür Sicherheitsexperten nötig sind. Da nicht automatisiert, ist die Sicherheitslösung bei jedem neuen Release oder bei einer Erweiterung des Systems mit dem entsprechenden Aufwand neu zu überprüfen.

Die Maturität der Sicherheitssysteme hat nicht mit der rasanten technischen und wirtschaftlichen Entwicklung Schritt gehalten. Die Lücke zwischen günstiger Kommoditisierung – digitale Infrastrukturen versprechen Effizienz und Benutzerfreundlichkeit – und nötiger Sicherheit wird grösser.

4.2.1.5 Organisch gewachsene Systeme

In vielen Organisationen sind die digitalen Infrastrukturen organisch gewachsen, wodurch noch viele Anwendungen und Systeme aus der Pionierzeit der IKT-Entwicklung am Laufen sind. Man zögert, sie zu ersetzen oder in eine moderne sicherere IKT-Umgebung zu migrieren, weil dies kurz- und mittelfristig hohe Kosten und Verfügbarkeitsausfälle zur Folge haben kann. Bereits die Wartung dieser Systeme stellt die Organisationen vor Probleme, insbesondere aber die Überführung der Daten und Prozesse in ein völlig neues System. In der Regel werden durch die Digitalisierung Kostenersparnisse, zusätzlicher Nutzen und nicht steigende Kosten erwartet. Der Ansatz hat sich eingebürgert „If it ain't broke, don't fix it“, was eine Industrialisierung der Sicherheit verhindert und langfristig in ein Sicherheitsproblem münden muss. Die organisch gewachsenen digitalen Systeme widerspiegeln sich in der Organisationsstruktur selbst. Statt eines zentral umgesetzten IT-Business-Security Alignement Prinzips (effiziente Verzahnung von IKT- und Geschäftsprozessmanagement mit Berücksichtigung des Risikomanagements), das in der entsprechend adaptierten Unternehmensarchitektur verankert ist, sind immer noch unkoordinierte Verantwortlichkeiten und Entscheidungsstellen anzutreffen.

4.2.1.6 Informationstheoretische und mathematisch komplexitätsbasierte Sicherheit

Bei der sogenannten informationstheoretischen Sicherheit („Information theoretical Security") hat der Angreifer zu wenig Informationen, um die Verschlüsselung zu entziffern. Selbst mit unbegrenzten Computerrechenressourcen lässt sich eine solche Verschlüsselung nicht brechen. Zu diesen aus mathematischer Sicht sicheren Verschlüsselungsmechanismen gehören unter anderem die Quantenkryptografie und unter speziellen Voraussetzungen die symmetrische Verschlüsselung. Deren Anwendung ist aber ressourcenintensiv und im Alltagsgebrauch nicht benutzerfreundlich genug.

Bei der sogenannten „Complexity-based Security“ hingegen stützt sich die Verschlüsselung auf mathematische Probleme. Diese Anwendungen haben sich durchgesetzt und im Alltag bewährt. Es ist aber nur eine Frage der Zeit, bis sie durch Rechenleistung oder neue mathematische Durchbrüche keinen genügenden Schutz mehr liefern werden (s. Ziff. 4.4.1).

4.2.1.7 Dilemma zwischen Komfort und Sicherheit

Die zwei verschiedenen Ansätze bei der Kryptografie zeigen exemplarisch das Dilemma zwischen Sicherheit und Komfort/Alltagstauglichkeit. Nach wie vor werden mehrheitlich die letzteren priorisiert. Die Erfahrung im Wirtschaftsbereich zeigt: Wenn die finanziellen Mittel für die IKT reduziert werden, zum Beispiel durch Sparmassnahmen, und die Dienstleistungen ohnehin eingeschränkt werden, ist die Geschäftsseite in der Regel nicht bereit, zusätzliche Opfer in Bezug auf die Funktionalität auf sich zu nehmen, um die Sicherheit zu verbessern. Nicht anders sieht es im privaten Bereich aus. Wenn die digitale Infrastruktur, sei es eine Applikation oder ein Gegenstand aus der IoT-Welt, wie etwa ein Fernsehgerät, vernetzt funktioniert und seinen Dienst erfüllt, werden Sicherheitsaspekte kaum noch verfolgt.

4.2.1.8 Der Faktor Mensch

Private, aber auch professionelle Nutzerinnen und Nutzer erwarten immer mehr Komfort und „coole“ neue digitale Dinge. Die Faszination für das Mögliche hält ungebremst

an. Obwohl man mittlerweile tagtäglich in den Medien auf das Thema digitale Sicherheit stösst, scheint diese nach wie vor zweitrangig zu sein, was zum Beispiel verschiedene Auswertungen über die Wahl von Passwörtern zeigen: Menschen tendieren dazu, immer wieder die gleichen Passwörter zu verwenden. Der unbegrenzte digitale Sturm und Drang hat nur begrenzt die Lernbereitschaft erhöht. Wovor die Sicherheitsexperten bei der Revolution der IoT gewarnt haben, ist längst eingetreten. Man wiederholt die gleichen Fehler und Unachtsamkeiten wie bei der Vernetzung der Computer vor über 20 Jahren. Es ist zu beobachten, dass die Awareness steigt, aber mit einem zwiespältigen Ergebnis. Sie führt einerseits zu mehr Befähigung und Verantwortungsbewusstsein bei den Nutzerinnen und Nutzern. Andererseits ist aber auch Überforderung und eine Art Ohnmacht und Desinteresse feststellbar. Die digitale Transformation läuft Gefahr, beim nächsten Schritt zum „Internet of Everything“ (IoE) – und darunter fällt u.a. auch die Vernetzung des Menschen mittels Implantaten (Herzschrittmacher, Sensoren, neuartige Maschine-Mensch-Schnittstellen) – die gleichen Fehler aus den gleichen Gründen noch einmal zu machen, obwohl das Risiko dann deutlich ansteigen wird. Sicherheits- und Verantwortungsbewusstsein scheinen an ihre Grenzen zu stossen. Umso mehr muss die Bevölkerung befähigt und müssen die Produzenten und Anbieter digitaler Dienste und Produkte in die Verantwortung einbezogen werden.

4.2.1.9 Der Faktor Wirtschaft

Im Sog der digitalen Transformation kommen auch informatikferne Unternehmen nicht mehr darum herum, digitale Ökosysteme im Vertrieb und im Betrieb auf- und auszubauen. Gemäss einer Studie zur Digitalisierung in Schweizer KMU betreiben bereits knapp drei Viertel der befragten Betriebe Digitalisierungsprojekte. Die gleiche Studie zeigt auch, wo die Risiken der Zukunft liegen: Die grosse Mehrheit der Unternehmen sieht das fehlende Knowhow und den hohen Investitionsbedarf als zentrale Herausforderungen. Insbesondere kleinere und mittlere Betriebe sind davon betroffen, da sie nicht über die entsprechenden IKT-Abteilungen verfügen und ihre Gewinnmargen die hochpreisigen Dienstleistungen von IKT-Security-Dienstleistern nicht finanzieren können. Da die KMU das Rückgrat der Schweizer Wirtschaft bilden, ist diesem Umstand besondere Beachtung zu schenken: Mehr als 99 % der Unternehmen sind kleinere und mittlere Unternehmen (1-250 Mitarbeitende), die zwei Drittel der Arbeitsplätze schaffen und einen bedeutenden Anteil am BIP erwirtschaften.

Auf der anderen Seite sind die Entwickler und Anwender unter ständigem Druck, als erste auf dem Markt zu sein, und hohe Erneuerungszyklen einzuhalten. Beides ist ihnen weit wichtiger, als „Sicherheit“ auf den Markt zu bringen. Kleine, aber auch grosse Unternehmen können sich Codeanalysen und Verwundbarkeitsüberprüfungen aufgrund des Zeitdrucks nicht leisten. Zudem kommt hinzu, dass gerade im IoT-Markt bei den Massenprodukten mit einer globalen Konkurrenz die Gewinnmargen zu klein sind, um diese Mehrkosten aufzufangen. Hier spielt wieder der Faktor Mensch eine Rolle, der sich unter Informationssicherheit bei digitalen Geräten wenig vorstellen kann und sie deshalb auch nicht als Qualitätsmerkmal erkennt. Auch hier ist der Staat in Zusammenarbeit mit den Produzenten und Anbietern gefordert, für mehr Sicherheit zu sorgen. Awareness-Kampagnen beim Anwender sind genauso nötig wie die Diskussion über neue Bestimmungen bei der Haftung, Zertifizierungsvorschriften bei Produkten und Dienstleistungen und bei den Normen respektive Standards bei der Organisationsführung.

4.2.2 Angriffsfläche wird grösser

Immer mehr Bereiche stützen sich auf digitale Infrastrukturen ab – die Folge der Allgegenwart von Computern und Netzen („ubiquitous Computing"). Da diese verwundbar sind, überträgt sich die Verwundbarkeit auf alle Gebiete, die von der digitalen Transformation durchdrungen werden. Wurden in den 1990er-Jahren des letzten Jahrhunderts nur Computer, in den frühen 2000er-Jahren zusätzlich mobile Geräte wie Laptops, Smartphones und Tablets vernetzt, spricht man heute vom IoT. Von komplexen Produktionsinseln in Unternehmen bis zur Zahnbürste werden heute alle Dinge Teil des (Inter-)Netzes, weil es Bedienungskomfort, Automatisierung, Kontrolle, Wartung und Effizienz verbessert. Für Aufsehen haben 2017 Sicherheitswarnungen gesorgt, die vor Cyberangriffen auf mit dem Internet verbundene Defibrillatoren, Herzschrittmacher, Insulinpumpen etc. warnen. Dieses sogenannte „Internet von Allem", macht auch vor dem Menschen nicht halt. Die Angriffsfläche wird immer grösser und die Datenflüsse zwischen den „Dingen" unkontrollierbarer und verwundbarer. Beschränkte sich das Risiko früher auf die virtuelle Welt, ist heute die physische Welt gleichermassen betroffen.

4.2.3 Schadenspotenzial wächst

Den digitalen Infrastrukturen werden immer mehr Aufgaben übertragen, die kritische und sensitive Daten beinhalten. Ob nun Herzschrittmacher oder kritische Infrastrukturen wie Gesundheitswesen, Finanzwesen, Energie und Sicherheitsdienste – bei Zwischenfällen stehen auch Leib und Leben auf dem Spiel. Die Cyberangriffe auf Spitäler zeigen, dass die Angreifer in keiner Weise davor zurückschrecken, auch solche Infrastrukturen anzugreifen. Ebenso wären Umweltkatastrophen vorstellbar, wenn Cyberzwischenfälle, z.B. bei Chemieunternehmen, ausser Kontrolle geraten würden.

Der Angriff auf den von Swift abgewickelten Interbanken-Zahlungsverkehr im Jahre 2016 macht deutlich, welchen Schaden professionelle Cyberangriffe selbst auf gut geschützte zentrale Systeme anrichten können. Im IoE kann alles - vom Computer bis zum Menschen - einen Schaden erleiden. In Zukunft dürften durch die zunehmende Vernetzung auch die Quantität der Fälle und die entsprechenden Schäden zunehmen.

Das verheerende Schadenspotenzial sogenannter systemischer Angriffe, die flächendeckend digitale Infrastrukturen lahmlegen, war in letzter Zeit vermehrt Thema von Diskussionen. Tatsächlich käme das Szenario eines Zusammenbruchs grosser oder kritischer Teile der digitalen Infrastruktur infolge eines systemischen Cyberangriffs einem „Cybergeddon" gleich mit entsprechenden Folgen für die gesamte Gesellschaft und Weltwirtschaft. Doch gerade der grösste Cybervorfall der letzten Jahre mit systemischen Folgen, WannaCry, mit über 400 000 betroffenen Systemen in über 150 Ländern zeigt die Grenzen des Schadenspotenzials auf. Dieser Vorfall war zwar punktuell verheerend, aus systemischer Sicht aber unbedeutend. Selbst bei weit benutzten Soft- und Hardwarelösungen wie z.B. SAP, Windows und Chips von Intel führen die Vielfalt der kontextbezogenen verbraucherspezifischen Einstellungen und die verschiedensten Versionen zu keiner eigentlichen Monokultur, bei der ein Schädling einen systemischen Schaden anrichten könnte. Obwohl aufgrund der technischen Revolution nichts ausgeschlossen werden kann, dürfte sich die Risikoeinschätzung auch mittelfristig nicht ändern. Der heutige Stand der unausgereiften Industrialisierung bzw. Standardisierung der Hard-, insbesondere aber der Software, bringt zwar Nachteile mit sich (s. weiter unten Bedrohungen), schützt aber auch durch seine Diversität vor solchen Angriffen. Langfristig dürften Standardisierung und Zentralisierung der digitalen Infrastrukturen neue Angriffsmöglichkeiten eröffnen, der gleiche Fortschritt dürfte aber auch den Schutz und die Wartung solcher Systeme massgeblich verbessern.

Die Infrastruktur „Internet“ ist gesondert zu betrachten. Unter dem Aspekt des sogenannten Kill Switch (Internet Notausschalter) haben jedenfalls gewisse Staaten die Möglichkeit, zumindest für ihr Staatsgebiet das Internet lahmzulegen (s. auch Ziff. 4.4.3). Weitreichendere Abschaltungen wären zwar möglich, aber technisch anspruchsvoll und ressourcenintensiv und vorderhand nur bei Staatsakteuren vorstellbar.

4.2.4 Bedrohungen

In der „Cyberwelt“ liegen die Vorteile beim Angreifer. Dieser kann jederzeit angreifen, er setzt sich durch den Remote-Zugang keinem direkten Risiko aus, und er kann so lange Angriffsmuster testen, bis er Erfolg hat. Ganz anders bei den IKT-Sicherheitsverantwortlichen: Trotz der erfolgreichen Abwehr Tausender von Angriffen an einem Tag kann bereits ein Fehler am nächsten Tag verheerende Auswirkungen haben.

Die Professionalisierung auf der Angreiferseite nimmt zu. Man arbeitet arbeitsteilig, was die Möglichkeit zum Cyberangriff nicht mehr auf Spezialisten einschränkt. Dank „Cyber-Attack as a Service“ (auch: „Cybercrime as a Service“) erhält jeder zahlungswillige Akteur im Darknet ausgeklügelte und massgeschneiderte Dienstleistungen. Die Angriffsinstrumente werden immer ausgereifter, während gleichzeitig sinkende Preise zu beobachten sind, wie etwa bei DDoS. Solche Angriffsressourcen kann man bereits für wenig Geld im Netz mieten. Insgesamt sind die technischen Eintrittshürden für Kriminelle deutlich gesunken. Die Zahlen, soweit verlässlich, sprechen eine deutliche Sprache; Kriminalität und Spionage sind mittlerweile die dominierende Motivation für weit über drei Viertel aller Cybervorfälle. Die Angriffe mit kriminellem Hintergrund sind gegenüber 2015 sprunghaft angestiegen.

Infolge „Cyber-Attack as a Service“ kommen immer häufiger mehrschichtige Angriffe zur Anwendung. DDoS-Angriffe dienen zum Beispiel dazu, von der Korruption anderer Systeme abzulenken mit dem Ziel der Datenexfiltration. Gleichzeitig werden mehrere Angriffsinstrumente (blended Threats) wie Viren, Trojaner, „social Engineering“ und Schwachstellenattacken gegen die identifizierten Verwundbarkeiten benutzt.

Auch die Nachrichtendienste haben die Vorzüge der virtuellen Welt entdeckt und investieren bedeutende Mittel in Angriffswerkzeuge. Staatlich geförderte und unterstützte Technologiespionage nimmt zu. So waren bis vor ein paar Jahren sogenannte „advanced persistent Threats", anhaltende auf spezifische Ziele zugeschnittene Angriffsinstrumente (alle Arten von Schadsoftware) und vor allem die „Zero-Day Exploits" staatlichen Akteuren vorbehalten. Beinahe 90 % der neu erkannten Malware wird nur einmal bei einem spezifischen Angriff verwendet, was die automatisierte Erkennung erschwert.

Früher sorgsam von Nachrichtendiensten und Militär gehütet haben diese heiklen Cyberangriffswaffen in den letzten zwei Jahren durch Datenlecks bei den Nachrichtendiensten den Weg an die Öffentlichkeit und ins Darknet gefunden. In gewissen Staaten gelangen solche Cyberwaffen in die Hände von Cyberakteuren, die für den Staat arbeiten, ihr Wissen und die Instrumente aber auch für kriminelle Zwecke anwenden. Damit wird die Unterscheidung zwischen staatlichen und staatsnahen Akteuren immer schwieriger.

Obwohl die Gefahr von Ransomware oder der Angriff auf den Zahlungsverkehr auf allen Ebenen in aller Munde ist, dürfte insbesondere der Handel mit gestohlenen Daten (Technologieinformationen, Geschäftsgeheimnisse, Gesundheitsdaten, Staatsgeheimnisse etc.) weiter zunehmen.

Nicht nur die Angriffsvehikel, sondern auch die Verdienstmöglichkeiten haben sich massiv erhöht: Die ganze cyber-kriminelle Wertschöpfungskette hat sich globalisiert und professionalisiert. Neben den erwähnten „Darknet Services“ vereinfachen organisierte Datenmärkte im Darknet die Ökonomisierung der verschiedenen Geschäftsmodelle. So ist es nicht erstaunlich, dass die organisierte Kriminalität das Potenzial im Cyberraum nutzt und davon profitiert, dass die Sicherheitsmassnahmen das Niveau der physischen Welt noch nicht erreicht haben

Dass Angriffe auf die Verfügbarkeit von digitalen Infrastrukturen und Daten sehr schnell offenkundig werden, liegt auf der Hand: Dabei ist alles möglich und bereits geschehen, von der feindlichen Verschlüsselung der Daten durch Ransomware bis zur Störung oder Zerstörung ganzer Industrieanlagen, etwa eines Hochofens in Deutschland. Weitaus schwieriger ist es dagegen, das Risikoausmass des ungewollten Datenabflusses zu bewerten. Kundendaten, wichtige Geschäftsdaten, geistiges Eigentum und Benutzeranmeldeinformationen können davon betroffen sein. Die Zeitdauer zwischen Infektion und Detektion bei einem erfolgreichen Angriff wird immer länger – aktuell gehen die Schätzungen der Experten von über 270 Tagen aus. Brisant ist zudem, dass die meisten Angegriffenen erst von externen Partnern gewarnt werden mussten. Der Angriff auf die Vertraulichkeit von Daten dürfte in Zukunft noch deutlich zunehmen. Die Vorteile sind offensichtlich: Der Angreifer dringt in ein System ein, hinterlässt nach Möglichkeit keine Spuren, kopiert die Daten und verschwindet. Dies erschwert die Suche nach der Täterschaft und deren Verfolgung und Bestrafung weiter.

Wenn man davon ausgeht, dass Experten mit den entsprechenden Ressourcen die Grundstruktur der Systeme beim heutigen Sicherheitspotenzial korrumpieren können und die Datenexfiltration nicht präventiv verunmöglicht werden kann, wird die Resilienz im Bereich der Detektions- und der Kontrollmöglichkeiten immer wichtiger. Insbesondere der Staat, aber auch Forschung und Wirtschaft im Hochtechnologiebereich müssen sich im Klaren sein, dass ihre Systeme bereits korrumpiert sind bzw. früher oder später korrumpiert werden und ein Datenabfluss möglich ist.

Die Informationssicherheit hat in den letzten Jahren grosse Fortschritte gemacht. Nichtsdestotrotz hat das Gesamtrisiko angesichts der betroffenen sensitiven und kritischen Prozesse und Daten sowie der gestiegenen Bedrohung zugenommen. Es hat Jahrhunderte gebraucht, bis die physische Sicherheit den heutigen Sicherheitsstandard erreicht hat. Soviel Zeit hat die moderne Gesellschaft nicht. Wenn Expertinnen und Experten Jahrzehnte für die Lösung der Probleme veranschlagen, ist dies deutlich zu lang.

4.3 Bildung, Kompetenz, Organisationen

4.3.1 „Informatiker-Autismus“

Informationssicherheit ist ein komplexes und mittlerweile hochgradig interdisziplinäres Gebiet, wo Informatiker u.a. mit Juristen oder Geschäftsprozessanalysten zusammenarbeiten müssen. Der Datenschutz ist ein Musterbeispiel dafür, dass nur Multidisziplinärität zum Ziel führen kann. Denn das Unvermögen von Rechts-, Risiko-, Compliance- und Informatikexpertinnen und -experten, eine gemeinsame Sprache zu finden und ein gemeinsames Problemverständnis zu entwickeln, wiegt mindestens so schwer wie Mängel bei der Grundsicherheitseinstellung.

Ein anderes Feld ist das IoT, bei dem Informatiker, IKT-Security-Spezialisten, Business-Experten und Ingenieure zusammenarbeiten müssen. Die fehlende Kommunikation zwischen den Expertensilos stellt eine Verwundbarkeit dar. Die heutige Informatik-Ausbildung geht hingegen immer noch davon aus, dass Informatik-Spezialisten im geschlossenen Silo für digitale Probleme digitale Lösungen suchen und den Austausch nach aussen nicht brauchen. In einer Welt des IoE stellt ein solcher "Informatiker–Autismus" eine Gefahr dar. Die Lehrgänge müssen deshalb entsprechend ergänzt werden mit Schulung im Bereich der mündlichen und schriftlichen Kommunikation, damit die Informatiker ihre Gestaltungskompetenz in Zusammenarbeit mit allen anderen wahrnehmen können. (s. auch Ziff. 10.3)

4.3.2 Es fehlt an Informationssicherheitsexperten

Bereits heute fehlt es an Informationssicherheitsexpertinnen und -experten, und zwar von security-sensibilisierten Programmierern bis hin zu „Chief Information Security Officer" (CISO) und Datenschutzbeauftragten mit dem nötigen juristischen, aber vor allem auch technischen Wissen. Diese Lücke wird im Verlauf der digitalen Transformation noch grösser werden.

Viele Ursachen haben zu dieser Situation geführt: Es fehlt an Lehrabteilungen für Informationssicherheit an den Eidgenössischen Technischen Hochschulen, den Universitäten und den Fachhochschulen. Ebenfalls fehlt es an einer anerkannten Zusammenstellung von Lerninhalten, die ein Curriculum für Informationssicherheit mit entsprechenden Abschlüssen (z.B. „digital Trust") definiert, vergleichbar mit dem Master für „Data Science". Entsprechende Projekte sind erst kürzlich im ETH-Bereich (ETH/EPFL) und an der Fachhochschule in Luzern angelaufen. Die Bildungseinrichtungen sind gefordert, ihre Anstrengungen in diesem Bereich zu intensivieren und ein gemeinsames Verständnis über die nötigen Lerninhalte zu entwickeln. Das Fehlen von Lehrabteilungen, Fachdozierenden und eines klaren Ausbildungsprofils führen dazu, dass sich Studierende nicht angesprochen fühlen.

4.3.3 Informationssicherheit als Teil der Grundausbildung

Es fehlt aber auch auf der Nicht-Informatiker-Seite an Wissen, die digitale Entwicklung und das Thema Sicherheit zu verstehen. Dieses Wissen muss im Grundstudium u.a. von Juristen, Medizinern, Ingenieuren und Gesellschaftswissenschaftlern eingebettet werden, ebenso in der Berufsausbildung (ähnlich dem MBA, das alle Nicht-Ökonomen für die Wirtschaftswelt befähigen soll).

Bei der nötigen Wissensvermittlung geht es nicht nur um das Programmieren, sondern um Grundlagen wie „computational Thinking", „Computer Literacy" und ein Grundverständnis für das Zusammenspiel grundlegender Elemente wie Netzwerke, Betriebssysteme und Applikationen und Grundlagen der Stochastik (s. auch Ziff. 10).

4.3.4 Sensibilisierung und das Wissen um die Gefahren: Informationssicherheit als Teil der Allgemeinbildung

Auch im digitalen Ökosystem kann die Sicherheit nur so gut sein, wie das schwächste Glied in der Kette; d.h. die einzelne Person. Wer sich nicht schützt, gefährdet auch andere. Sensibilisierungskampagnen und Ausbildungsprogramme für alle Mitglieder der Gesellschaft sind nötig und bis jetzt zu wenig zum Einsatz gekommen.

1. Empfehlungen:

- Der Bund setzt sich dafür ein, dass die Eidgenössischen Technischen Hochschulen, die Universitäten sowie die Fachhochschulen und Berufsbildungsinstitutionen mit Ausbildungsangeboten im Bereich der IKT die Informationssicherheit ausbauen und vernetzen und die dafür minimal notwendigen Lerninhalte festlegen;
- dass die Informationssicherheit bei den Eidgenössischen Technischen Hochschulen, den Universitäten sowie den Fachhochschulen und Berufsbildungsinstitutionen Teil der Grundausbildung wird.

4.4 Vertiefungsthemen

4.4.1 Zukunft der Kryptografie

Wesentliche Sicherheitsinstrumente im Ökosystem Internet beruhen auf Verschlüsselungstechniken, die auf mathematischer Komplexität beruhen. Sie ermöglichen sichere Netzwerkverbindungen u.a. zwischen dem Browser und einer Internetseite, das Authentifizieren von natürlichen (u.a. E-ID), juristischen und technischen Entitäten, das digitale Signieren oder auch die Verschlüsselung von Textnachrichtendiensten. Sie bilden das Rückgrat des Vertrauens und der Integrität im Netz.

Der asymmetrischen Verschlüsselung kommt beim digitalen Signieren und Verschlüsseln eine besondere Bedeutung zu, da sie im Unterschied zur symmetrischen Verschlüsselung ein einfaches und sicheres Schlüsselmanagement erlaubt. Bei der symmetrischen Verschlüsselung müssen die Nutzerinnen und Nutzer den Schlüssel auf einem anderen Kanal direkt austauschen. Bei jeder Anpassung des Adressatenkreises muss somit ein neuer Schlüsselaustausch stattfinden. Bei vielen Nutzern im gleichen System steigt das Risiko, dass die Vertraulichkeit der Schlüssel korrumpiert wird.

Bei der asymmetrischen Verschlüsselung entfallen diese Probleme dank einer public Key-Infrastruktur (PKI), da der öffentliche Schlüssel für die Verschlüsselung und Verifikation von digitalen Signaturen die Ableitung des privaten Schlüssels für Entschlüsselung oder Signaturerstellung nicht zulässt. Die Bekanntmachung der öffentlichen Schlüssel ist deshalb ein Hauptmerkmal der asymmetrischen Kryptografie.

Ein Beispiel soll dies erläutern. Der öffentliche Schlüssel eines Web-Servers ist öffentlich bekannt. Sobald der Browser einer Nutzerin oder eines Nutzers eine Verbindung zu diesem Web-Server aufbaut, prüft er die Identität des Web-Servers anhand eines von einer dritten Instanz erstellten Zertifikats und schlägt dem Webserver einen symmetrischen Schlüssel vor, den er mit dem öffentlichen Schlüssel des Webservers verschlüsselt (z.B. durch das RSA-System). Komplett automatisiert und im Hintergrund wiederholt sich dieser Vorgang zigmilliardenfach bei jedem als „https“ bezeichneten sicheren Verbindungsaufbau.

Die sogenannten Hash Algorithmen gehören ebenfalls zu den kryptografischen Verfahren. Hashwerte sind mathematisch hergeleitete Prüfsummen von einem beliebigen Wert. Werte können Nachrichten, Text oder zum Beispiel Passwörter sein, die auf eine Prüfsumme mit festgelegter Länge mittels eines Algorithmus umgerechnet werden. Der Sicherheitsalgorithmus ist erstens so angelegt, dass von der Prüfsumme der Ausgangswert nicht zurückgerechnet werden kann, und zweitens so, dass es praktisch unmöglich ist, neben einem gegebenen Wert einen anderen Wert zu generieren, der den gleichen Hashwert ergibt.

Nicht nur die Sicherheit im Internet, auch andere mittlerweile digitale Infrastrukturen wie die Blockchain beruhen auf der Technologie der asymmetrischen Verschlüsselung und von Hashwerten. So ist Blockchain eine Aneinanderreihung von signierten Transaktionen, die „gehasht“ werden (s. Ziff. 9.1.4).

Als in den 1970er-Jahren des 20. Jahrhunderts die gängigsten asymmetrischen Systeme wie RSA eingeführt wurden, ging man von einem Sicherheitshorizont von Jahrhunderten aus. Angesichts der Entwicklung der Quantencomputer und möglichen Durchbrüchen in der Mathematik ist man sich heute der Tatsache bewusst, dass auf mathematischer Komplexität basierende Sicherheitssysteme diesem Zeithorizont nicht gerecht werden können. In der Folge wären nicht nur die Vertraulichkeit und die Integrität der aktuellen Datenverarbeitung gefährdet, sondern alle bis dahin verschlüsselten Daten. Die heutigen auf asymmetrischer Verschlüsselung beruhenden Sicherheitssysteme sind daher eine tickende Zeitbombe. Bei der symmetrischen Verschlüsselung wie etwa AES (Advanced Encryption Standard), reicht hingegen eine entsprechende Verlängerung der Blockgrösse, um sie gegen Quantencomputer-Angriffe zu schützen.

Technologische Alternativen stehen bereits heute zur Verfügung, sind aber weit davon entfernt, in die tägliche Praxis umgesetzt zu werden. Zudem brauchen grundlegende Änderungen im Ökosystem Internet viel Zeit. So ist beispielsweise der Austausch des Hashing Algorithmus MD5, bei dem im Jahr 2004 signifikante Schwachstellen entdeckt worden sind, immer noch nicht vollständig abgeschlossen.

Zu den Alternativen gehören sogenannte Postquantum-Algorithmen, die auf mathematischen Problemen basieren, von einem Quantencomputer aber gemäss heutigem Kenntnisstand nicht gelöst werden können. Vielversprechende Ansätze für einen solchen asymmetrischen Verschlüsselungsalgorithmus sind das McEliece-System oder das NTRUEncrypt. Schliesslich ist aber allen Überprüfungen gemeinsam, dass zurzeit noch kein voll funktionsfähiger Quantencomputer zur Verfügung steht, um die Sicherheit oder Unsicherheit dieser Ansätze auch in der Praxis zu verifizieren.

Da davon auszugehen ist, dass alle auf mathematischer Komplexität basierenden Ansätze eines Tages angreifbar werden - in zehn bis fünfzehn Jahren dürften Quantencomputer die heute gängigen asymmetrischen Verschlüsselungen brechen -, bringt dies enorme Herausforderungen mit sich: Bei jedem Wechsel auf einen neuen Verschlüsselungsalgorithmus müssten alle bisherig verschlüsselten Daten umverschlüsselt werden. Beim heutigen Stand der Technik und Organisation ist dies mit einem verhältnismässigen wirtschaftlichen Aufwand nicht realisierbar. Noch schwerer wiegt das Risiko, dass Daten, die nach dem Prinzip „kopiere jetzt, entschlüssle später“ („store now decode later“) entwendet wurden, jeder Kontrolle entzogen sind. Eine Umverschlüsselung bringt nur unter der Voraussetzung einen Mehrwert, dass die Angreifer die Daten nicht bereits zu einem früheren Zeitpunkt abgegriffen haben.

Das Szenario eines digitalen Ökosystems ohne Lösung für die Postquantumkryptografie wird regelmässig als das noch denkbare schlimmstmögliche Cyberszenario bezeichnet. Bei Schutz- und Sperrfristen, wie etwa bei der Akteneinsicht auf Bundesebene gemäss Archivierungsgesetz vom 26. Juni 1998 (BGA), die 30 bzw. bei besonders schützenswerten Personendaten 50 Jahre und zumindest bis zum Tod betragen, werden die Zeitdimensionen und die Ansprüche an die Vertraulichkeit und Integrität von Daten ersichtlich.

Nur informationstheoretisch sichere Verschlüsselungstechniken garantieren langfristige Sicherheit für einen Zeithorizont von 100 Jahren. Dazu gehört die physische Verteilung kryptografischer Schlüssel auf Basis des Quantenschlüsselaustausches. Vor diesem Hintergrund setzen sich verschiedene Staaten wie die USA und Deutschland, aber auch die EU intensiv mit der Postquantumkryptografie auseinander und haben

entsprechende Gremien und Arbeitsgruppen eingesetzt. Angesichts der langen Adaptionszeit sind frühzeitig praxistaugliche Lösungen zu evaluieren und deren Implementierung zu planen. Auch die Schweiz muss diese Herausforderung vertieft und angesichts der langen Umsetzungszeiten frühzeitig an die Hand nehmen.

Schliesslich hängt die Güte einer Verschlüsselung wesentlich von der Wahl des Zufallszahlengenerators ab. Physikalische Zufallszahlengeneratoren wie z.B. Quantensprünge bieten einen höheren Schutz bei der Erzeugung der Schlüssel und damit auch bei der Verschlüsselung als softwaregestützte Pseudozufallszahlengeneratoren. Pseudozufallszahlengeneratoren sollten vermieden werden. Die Kosten für solche Systeme fallen angesichts immer grösserer Märkte und sind mit den Ansprüchen an die Sicherheit kompatibel.

4.4.2 Sicherheit der Datenbearbeitung

Die Datenbearbeitung kennt drei Zustände: Während der Speicherung (Data at Rest), während der Übertragung (Data in Transit) und während der Verarbeitung (Data in Use). Für den Schutz sind bei allen drei Zuständen kryptografische Techniken notwendig.

Daten während der Übertragung (Data in Transit)
Die Datenverschlüsselung bietet den nötigen Schutz bei der Übertragung von Daten, wofür ein Schlüsselverteilungssystem für die kommunizierenden Parteien nötig ist. Da die heute gebräuchlichen asymmetrischen Systeme langfristig nicht sicher sind, braucht es andere Lösungen. Ein informationstheoretisch sicheres System, das auch in Zukunft nicht angreifbar ist, beruht auf der Quantenschlüsselverteilung. Solche physikalischen Systeme sind bereits in der Schweiz kommerziell erhältlich. Wie bei den kryptografischen Schlüsselaustauschsystemen erfolgt die eigentliche Verschlüsselung mit der symmetrischen Verschlüsselung, z.B. AES-256, da diese eine effizientere Nachrichtenübermittlung ermöglicht.

Quantenschlüsselverteilungssysteme können auf den Standard-Glasfaserkabeln der Telekommunikation betrieben werden. Selbst ein paralleler Betrieb auf den gleichen Glasfasern wie die übrige Datenkommunikation ist möglich. Aus praktischen Gründen wird jedoch eine dedizierte Glasfaser für das Quanten-Signal verwendet. Diese Glasfaser muss aber nicht in einem separaten Kabel, sondern kann zusammen mit den Hunderten von Glasfasern für die anderen herkömmlichen Kommunikationszwecke verlegt werden. Dieser Photonik-Quanten Kanal muss durchgängig End-to-End verlaufen. Der heutige Stand der Technik erlaubt eine Reichweite von rund 100 km, bevor das Quanten Signal schwächer wird. Dies reicht aus, um in der Schweiz die Städte zu verbinden. In grösseren Städten würden vom Staat administrierte Knotenpunkte eingerichtet werden, welche die Weiterleitung über längere Distanzen sicherstellen. Die Knotenpunkte erlauben es den Behörden, die Kommunikation im Rahmen des Rechts zu überwachen.

Daten während der Speicherung (Data at Rest)
Neben den gängigen IKT-Schutzmassnahmen wie einem kohärenten Schlüsselmanagement (Prinzip der geringsten Zugangsrechte) und dem physischen Schutz der Server gehört insbesondere eine symmetrische Verschlüsselung der Daten zu den wirksamen präventiven Massnahmen. Für einen besseren Integritätsschutz der Daten müssen Protokolle wie das digitale Signieren mit einem Verfallsdatum versehen werden. Im Falle eines unerwarteten Fortschritts der Verschlüsselungsanalyse kann das Verfallsdatum entsprechend angepasst werden, damit die Daten neu signiert werden

müssen. Wie auch bei Data in Transit besteht die Gefahr, dass die Daten erst gestohlen und später entschlüsselt werden.

Daten während der Verarbeitung (Data in Use)
Die Bedrohung durch ein kompromittiertes Betriebssystem, bösartige Anwendungen oder kompromittierte Hardware machen den Schutz der Daten während der Bearbeitung zu einer Herausforderung.

Eine Möglichkeit ist die Anwendung von speziellen Prozessoren, die durch eine geschützte Programmausführungsumgebung (z.B. Enklave bei Intel Prozessoren) Schutz vor korrumpierten Betriebssystemen oder bösartigen Anwendungen bietet. Dies setzt allerdings das Vertrauen in die Hardwareproduzenten voraus, das angesichts korrumpierter Hardware und Verwundbarkeiten in den letzten Jahren arg in Mitleidenschaft gezogen worden ist. So beschäftigt sich die Forschung zurzeit eingehend mit Ansätzen, um Verwundbarkeiten und Hintertüren in der Hardware detektieren zu können – ein Forschungszweig, der in der Schweiz intensiviert werden müsste.

Eine andere Möglichkeit ist die homomorphe Verschlüsselung von Daten, die eine Bearbeitung erlaubt, ohne dass die Daten vorher entschlüsselt werden, und die sogenannte sichere verteilte Berechnung (secure Multi-Party Computation). Sie erlaubt es verschiedenen Parteien, den gleichen Berechnungsprozess zu benutzen, ohne dass die Dateneingaben oder die Zwischenergebnisse gegenüber den anderen Mitbenutzern ihre Vertraulichkeit verlieren. Dank homomorpher Verschlüsselung oder dem secure Multi-Party Computation könnte der Bearbeiter sensitiver Daten die Vorteile von Cloudservices nutzen, ohne einen hundertprozentig vertrauenswürdigen Cloud-Betreiber voraussetzen zu müssen.

Die Nachteile der homomorphen Verschlüsselungsanwendungen liegen in der limitierten Breite der verfügbaren Funktionalität, der dafür nötigen Rechenkapazität und der Langsamkeit der Prozessabwicklung, die eine operative kommerzielle Anwendung bisher verunmöglicht haben.

Schliesslich bauen die homomorphe Verschlüsselung und die „sichere verteilte Berechnung“ auf Grundsätzen der asymmetrischen Verschlüsselung auf, womit auch sie künftig durch Quantencomputer und neue mathematische Lösungen verwundbar sind. Um trotz dieser Verwundbarkeiten die Vorteile der Cloud zumindest in Ansätzen nutzen zu können, bleibt die symmetrische Verschlüsselung der Daten, die aber für jede Bearbeitung auf die eigenen Systeme zurückgeladen werden müssten. Dies ist dann zielführend, wenn die Daten nur gelegentlich bearbeitet werden, was der heutigen Entwicklung entgegenläuft, Daten und Prozesse ganzheitlich in die Cloud auszulagern.

Empfehlung:

2. Der Bund stellt in Zusammenarbeit mit den Kantonen sicher, dass die eingesetzte Verschlüsselungstechnik bei sensitiven Daten auch langfristig die notwendige Informationssicherheit gewährleistet. Die entsprechende Verschlüsselungstechnik soll allen privaten und öffentlichen Nutzerinnen und Nutzern zur Verfügung gestellt werden.

4.4.3 Ein hochsicheres Kommunikationsnetzwerk für die Schweiz

Als die Eisenbahn die Schweiz eroberte, brauchte es eine sichere landesweite Infrastruktur. Rund 100 Jahre später folgte der Siegeszug des Autos. Ohne ein nationales Engagement hätten diese Infrastrukturen nicht aufgebaut werden können. Das heutige

Internet verbindet weltweit Milliarden von Menschen und Geräten. Immer mehr Dienstleistungen und industrielle Prozesse hängen von der Internet-Kommunikation ab. Die Folgen eines Internetausfalls lassen erahnen, wie gross bereits die Abhängigkeit von dieser Infrastruktur geworden ist.

Aus diesem Grund braucht die Schweiz ein hochsicheres landesweites Kommunikationsnetzwerk, das die Kommunikation auch während aktiver Angriffe gewährleistet. Es muss den Inhalt der Informationen und die Identitäten der Absender und Adressaten sicherstellen und vor allem eine hohe Verfügbarkeitssicherheit aufweisen. Es dient einerseits dazu, die Kommunikation zwischen den Behörden auf allen Ebenen und den kritischen Infrastrukturen sicherzustellen und zwar auch in Krisenlagen. Andererseits gibt eine solche nationale Infrastruktur der ganzen Gesellschaft – und zwar Behörden, Unternehmen, Organisationen und Privatpersonen – die Möglichkeit, nach Sicherheitsbedarf und Ressourcen auf eine sichere Netzwerkkommunikation zurückgreifen zu können. Es ist davon auszugehen, dass bei einer zunehmenden Unsicherheit im offenen Ökosystem Internet der Bedarf nach einer solchen nationalen Infrastruktur zunehmen wird. Steht sie zur Verfügung, dürfte sie die digitale Transformation in der Schweiz nachhaltig fördern.

Ein wichtiger Aspekt ist die Internet-Souveränität. Das heutige Internet, und sogar die Netzwerk-Protokolle, welche sichere Kommunikation versprechen, weisen einen „Kill Switch“ auf, mit dem eine Grossmacht das Internet in einer Region ausschalten kann. Beispiele von solchen „Kill Switches“ sind DDoS-Angriffe, welche die Kommunikation verunmöglichen, oder „Route Hijacking" Angriffe, die verhindern, dass die Datenpakete den Weg zum Empfänger finden.

Wie im Kapitel zur Kryptografie (s. Ziff. 4.4.1) erläutert, beruhen die heute gängigen Sicherheitsinstrumente (Authentifizieren, Signieren, Transportsicherheit) im Netzwerk auf asymmetrischen Verschlüsselungstechniken, die langfristig keine Sicherheit garantieren. Insofern sind Ansätze zu prüfen, wie ein nachhaltig sicheres landesweites Kommunikationsnetzwerk aufgebaut werden kann. Dieses muss so weit wie möglich mit den jetzigen Kommunikationsprozessen kompatibel sein und allen interessierten Nutzern zur Verfügung stehen.

Ein traditioneller Ansatz für den Aufbau eines hochsicheren Netzes für die Schweiz könnte auf dedizierten Kommunikationsleitungen (Mietleitungen) wie MPLS, SDN oder SD-WAN beruhen. Diese Ansätze führen jedoch zu einem starren Netzwerk, das schwierig zu managen, zu erweitern und für mehrere Anbieter zu skalieren ist. Ein neuer Ansatz ist die SCION Netzwerk Architektur, welche die ETH Zürich entwickelt hat. SCION bietet Internet-Souveränität und garantiert auch bei Angriffen die Kommunikationsfähigkeit. Zudem ist SCION weitgehend mit den jetzigen Kommunikationsprozessen kompatibel und benötigt wenige Anpassungen an bestehenden Netzwerken.

Empfehlung:

3. Der Bund prüft in Zusammenarbeit mit den Kantonen die Möglichkeiten, privaten und öffentlichen Nutzerinnen und Nutzern ein sicheres und hoch verfügbares Kommunikationsnetzwerk zur Verfügung zu stellen.

4.4.4 Standards und Zertifizierungen von Produkten

4.4.4.1 Einführung

Die Zertifizierung ist ein Instrument, um darzulegen, dass Produkte, Dienstleistungen und Organisationen sich an definierte Anforderungen (Standards, Normen) halten und dies von einer dritten unabhängigen Partei geprüft ist.

Software und insbesondere cyber-physische Geräte weisen nach wie vor bedenkliche Sicherheitsmängel auf. Oft fehlt die notwendige Härtung gegen Angriffe. Die wichtigsten Härtungen sind: Die Möglichkeit, die Standardeinstellungen mit Benutzernamen und Passwort auf die Nutzerin oder den Nutzer zu spezifizieren, ein möglichst automatisiertes und lizenzgestütztes Updatesystem („Patching“) der eingebauten Software, entsprechend sichere Verschlüsselungslösungen bei IP-Telefonie, ein Virenscanner und ein eingebauter Ausschalte-Knopf („Kill Switch“). Der „Kill Switch“ erlaubt dem Produzenten oder einer Aufsichtsbehörde, das Gerät auszuschalten, wenn keine Updates mehr zur Verfügung stehen und das Gerät zu einer Gefahr wird – und dies nicht nur für die Nutzerin oder den Nutzer, sondern auch für andere, wenn das Gerät zum Beispiel als Teil eines Botnets als Mittel für einen IoT-DDoS Angriff missbraucht wird.

In der Schweiz haben sich Standards und Zertifizierungen bzw. Konformitätsbewertungen mit Bezug auf Softwareprodukte in verschiedenen Sektoren als Voraussetzung für die Marktzulassung bzw. das Inverkehrbringen von Produkten (z.B. bei Medizinprodukten und Fernmeldeprodukten) etabliert. Zu erwähnen sind in diesem Zusammenhang etwa auch der Schweizer Prüfungsstandard „Prüfung von Softwareprodukten" (PS 870) der Treuhandkammer sowie die den Standard konkretisierenden „RS-10 Grundsätze ordnungsgemässer Buchführung beim Einsatz von Informationstechnologie".

Allerdings sind auch die Herausforderungen nicht zu übersehen, wenn es um Prüfungsstandards für Software und cyber-physische Geräte geht. Digitale Funktionalität zeichnet sich durch eine hohe Flexibilität, Multifunktionalität und Kundenadaption aus. Zusätzlich hängt die Sicherheit der Software und der cyber-physischen Geräte massgeblich vom Kontext der digitalen Infrastrukturen ab, in denen sie die Nutzerin oder der Nutzer implementiert und den dabei vorgenommenen nutzerspezifischen Einstellungen. Die Konformitätsanforderungen müssten eine Vielzahl von Einstellungen abdecken, da jede Anpassung ein potenzielles Risiko darstellt. Die Umsetzung des statisch angelegten Zertifizierungsansatzes im dynamischen Softwareumfeld stellt eine besondere Herausforderung dar.

Die „Common Criteria for Information Technology Security Evaluation“ (CC) sind wohl der weitverbreitetste und anerkannteste Standard für die Überprüfung der Sicherheit von IKT-Produkten. Allerdings ist der Prüfprozess zeit- und kostenintensiv, weshalb er nur bei hochsensitiven Produkten wie etwa in der Raumfahrt zur Anwendung kommt. Der CC-Prozess zeigt exemplarisch, wie die Konformitätsüberprüfung mit Normen sehr schnell an ihre Grenzen stösst und unverhältnismässig wird, müsste doch bei jedem Update eines Geräts, zum Beispiel einer günstigen netzwerkfähigen Beleuchtung, der Prüfprozess von Grund auf wiederholt werden. Das Delta zwischen der Kommoditisierung von IKT-Produkten und fehlendem „Security by Design“ als Standard im B2C, aber auch im B2B-Bereich, zeigt sich hier in seinem ganzen Ausmass. Ein IKT-Produkte-Bezüger im Wirtschaftsumfeld kann die IKT-Sicherheit in seiner Produktionskette im Grunde genommen nur selbst überprüfen.

So erstaunt es nicht, dass beispielsweise die EU mit dem CE-Label für eine Vielzahl von Produkten eine Konformitätskennzeichnung durchgesetzt hat, die dem Benutzer einen harmonisierten Schutzlevel bezüglich Sicherheit und Gesundheit garantiert. Für Software oder cyber-physische Produkte fehlt bis jetzt eine solche Kennzeichnung.

4.4.4.2 Die Bedeutung von Zertifizierungen und Standards bei Haftungsfragen

Die offene Frage nach der Relevanz von Standards und Zertifizierungen von Produkten erschwert auch die Abgrenzung von Verantwortungsbereichen zwischen Nutzerinnen und Nutzern, verschiedenen Herstellern und Intermediären und damit auch die Beurteilung von haftungsrechtlichen Fragen delikts- und vertragsrechtlicher Natur (s. Ziff. 7.3.). Aus rechtlicher Sicht sind Standards und Zertifizierungen dann relevant, wenn deren Beachtung entweder einer generell oder zumindest in den beteiligten Kreisen (Branche) allgemein verbreiteten Praxis entspricht oder aber gesetzlich verbindlich vorgegeben ist. Die Nichteinhaltung von anerkannten Standards ist nach allgemeinen haftungsrechtlichen Grundsätzen als mangelnde Sorgfalt und damit als schuldhafte Fahrlässigkeit zu beurteilen, die, sofern die weiteren Haftungsvoraussetzungen gegeben sind (adäquater Kausalzusammenhang, Widerrechtlichkeit bzw. Verletzung einer vertraglichen Pflicht), zur Haftung für den aus der Missachtung des Standards resultierenden Schaden führt. Dabei dürfte allerdings insbesondere die Frage der Kausalität unter Umständen nicht ganz einfach zu beurteilen sein, wenn nämlich nicht von vorneherein eindeutig feststeht, dass bei Beachtung des Standards der eingetretene Schaden auf jeden Fall vermieden worden wäre.

Im Rahmen der Geschäftsherrenhaftung (Art. 55 OR) ist die Nichtbeachtung anerkannter Standards als Organisationsmangel zu beurteilen, der zur Haftung für den dadurch kausal und widerrechtlich verursachten Schaden führt. Im Zusammenhang mit der Produktehaftung stellt die Nichtbeachtung anerkannter Standards gegebenenfalls einen haftungsauslösenden Produktefehler dar.

Wenn die Beachtung eines bestimmten Standards bzw. die Zertifizierung nach einem bestimmten Standard gesetzlich vorgeschrieben ist, kann die Missachtung des Standards bzw. der Zertifizierungspflicht eine Widerrechtlichkeit darstellen.

Dies ist dann der Fall, wenn die gesetzlichen Bestimmungen zur verbindlichen Vorgabe von Sicherheitsstandards als sogenannte Schutznormen zu betrachten sind. Dies trifft zu, wenn der Zweck der betreffenden Bestimmung bzw. der Verbindlicherklärung eines bestimmten Standards darin besteht, potentiell Geschädigte gegen Schäden, die sich aus der Nichtbeachtung der gesetzlichen Vorgabe ergeben können, zu schützen. Soweit die Haftung dabei nach deliktsrechtlichen Grundsätzen zu beurteilen ist (der Schaden also nicht zwischen Vertragspartnern eingetreten ist), würde diese auch Schäden erfassen, welche nicht auf der Verletzung von absolut geschützten Rechtsgütern (Leib und Leben, Persönlichkeit, Eigentum) beruhen, da sich die Widerrechtlichkeit in diesen Fällen nicht aus der Verletzung absolut geschützter Rechte, sondern aus der Verletzung der gesetzlichen Schutznorm ergibt.

4.4.4.3 Haftung bei Anbietern von Zertifizierungsleistungen

Speziell zu prüfen ist die Frage der Haftung der Anbieter von Zertifizierungsleistungen für allfällige Schäden, welche Dritte erleiden, weil die Zertifizierung nicht ordnungsgemäss erfolgt ist. Falls keine spezifischen Haftungsnormen bestehen (wie sie z.B. für die Anbieter von Zertifizierungsdienstleistungen und für die Anerkennungsstellen von solchen Anbietern im Bundesgesetz vom 18. März 2016 über die elektronische Signa-

tur [ZertES] enthalten sind), gelten die allgemeinen deliktsrechtlichen Grundsätze (Verletzung von bei der Zertifizierung zu beachtenden Sorgfaltspflichten oder Verletzung von Schutznormen, z.B. gesetzlich definierten Zertifizierungsvoraussetzungen). In Frage käme allenfalls auch eine sogenannte Vertrauenshaftung (analog z.B. der Haftung im Zusammenhang mit Auskünften oder Gutachten), wenn nämlich die Erwerber eines Produktes auf eine Zertifizierung vertrauen und die Zertifizierungsdienstanbieter damit rechnen mussten, dass Dritte beim Erwerb des Produktes auf die Zertifizierung vertrauen, was regelmässig der Fall sein dürfte.

4.4.4.4 Schlussfolgerungen

Die Produktionsketten für IKT-Produkte sind global und von aussereuropäischen Akteuren dominiert: Vor diesem Hintergrund macht ein schweizerischer Alleingang mit einer Sicherheitsnormierung gegebenenfalls sogar mit Marktzulassungscharakter wenig Sinn. Hingegen sind entsprechende Modelle zu prüfen und zusammen mit der EU bzw. in internationalen Gremien weiterzuverfolgen. Ergänzend dazu könnten die Behörden - in Analogie zu den Reisehinweisen des EDA - eine Liste gefährlicher Software und cyber-physischer Geräte führen und so eine breite Informationsmöglichkeit schaffen (s. auch Ziff. 5.3.1.12).

Empfehlung:

4. Der Bund prüft in Abstimmung mit der Entwicklung im Ausland, ob und in welchen Bereichen Standards und Zertifizierungen zu einer Voraussetzung für den Marktzugang von IKT-Komponenten erklärt werden müssen, und welche gesetzlichen Rahmenbedingungen dafür nötig sind.

4.4.5 Massnahmen der guten Praxis, Normen und Standards

Die Entwicklung gängiger und erprobter IKT- und Informationssicherheitsstandards wurde hauptsächlich von grossen Unternehmen vorangetrieben. So verfolgen diese Frameworks, wie

- die ISO 27000 Familie,
- die vom Information Security Forum erarbeitete Information Risk Assessment Methodology 2 (IRAM2)IRAM,
- das von den USA für die kritischen Infrastrukturen entwickelte NIST Cybersecurity Framework (CSF) und SP 800-53 oder
- die vom BSI bereitgestellten Grundschutzkataloge (seit Februar 2018 aktualisiert bzw. ersetzt durch die BSI-Standards und das IT-Grundschutz-Kompendium)

einen ganzheitlichen systemischen Ansatz – oft noch mit der Implementierung eines detaillierten Risikomanagements. Andere kürzere Standards bzw. Guidelines wie jene der „International Chamber of Commerce: Cyber Security Guide for Business" sind wiederum nur als Einstieg für die Management Stufe geeignet oder so kurz gehalten, dass sie nur sehr grobkörnig eine erste einfache Checkliste vorschlagen (z.B. Infosurance oder Merkblatt für KMU von MELANI[6]), die lediglich das „Was“ skizzieren.

[6] https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html [Stand 10.5.2018] «Aus der Praxis - für die Praxis» KMU-Schriftenreihe. Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU).Das erweiterte 10-Punkte-Programm schafft mehr Schutz. 2016.

Was heute fehlt, ist ein kurzgefasster Leitfaden, der kleineren und mittleren Unternehmen, aber durchaus auch grösseren Betrieben den Weg zu mehr Sicherheit Schritt für Schritt aufzeigt.[7] Ein solcher Leitfaden hat folgende Zielsetzungen zu erfüllen:

Der Leitfaden soll die Nutzerinnen und Nutzer in die verschiedenen Verwundbarkeitsfelder digitaler Infrastrukturen einführen. Er berücksichtigt hierzu allgemeine sicherheitstechnische und organisatorische Aspekte sowie Fragen der Regelkonformität, geht aber auch auf einzelne wichtige Dienste wie E-Mail oder Web im Detail ein. Er schlägt drei Maturitätsebenen vor und hilft den Nutzern anhand von Checkfragen, ihren Sicherheitslevel zu finden. Auf jeder Ebene finden sich Sicherheitsmassnahmen, die konkret und nach Möglichkeit detailliert sind. Der oft angewendete technikneutrale Ansatz macht zwar angesichts der sich schnell entwickelnden Technik Sinn, erschwert aber auch die fassbare Festlegung von Sicherheitsniveaus. Insofern sind techniknahe Kriterien und Empfehlungen vorzuziehen. Dies setzt voraus, dass der Leitfaden von einer verantwortlichen Stelle konstant nachgeführt wird. Ein kurzer Kriterienkatalog hilft dem Nutzer zu entscheiden, wo sich ein Outsourcing/Managed Service anbietet. Der Leitfaden soll keine technische Einführung in die Informatiksicherheit sein – so führt er etwa nicht aus, wie ein Netzwerk Firewall zu konfigurieren ist. Er soll aber auditierbar sein und die Möglichkeit zur (Selbst-)Zertifizierung bieten.

Der Leitfaden soll Nutzer auf der Geschäftsleitungsstufe, aber auch auf der IKT-Administrator-Stufe befähigen, eine Maturitätsstufe festzulegen und von den IKT-Providern einzufordern. Auf einer gesamtgesellschaftlichen Ebene soll der Leitfaden als Grundlage für eine allgemein anerkannte good/best Practice, als Norm allenfalls auch für einen Standard dienen, sofern dies zum Beispiel bei den kritischen Infrastrukturen als angebracht erscheint. Breit abgestützt, anerkannt und umgesetzt trägt ein solcher Leitfaden dazu bei, ein gemeinsames Verständnis und eine Orientierung zu schaffen, wieviel Sicherheit im Cyberkontext durch Vorkehrungen verhältnismässig ist. Die Möglichkeit zur (Selbst-)Zertifizierung schliesslich trägt wesentlich dazu bei, im B2B- wie auch im B2C-Bereich durch Überprüfbarkeit und Transparenz ein Netzwerk des Vertrauens zu schaffen.

4.4.6 Digitale Identitäten

Neben der Infrastruktur für die asymmetrische Verschlüsselung bilden überprüfbare digitale Entitäten die Grundlage für die Sicherheit. Entitäten können natürliche und juristische Personen oder digitale Infrastrukturen sein. Die Basis für überprüfbare Identitäten sind Zertifizierungsstellen („Certification Authorities“, CA), die eine public Key-Infrastruktur betreiben und Zertifikate ausstellen. Solche Zertifikate beinhalten je nach Ausgestaltung verschiedene öffentliche-private Schlüsselpaare. Die Zertifikate sind durch den Aussteller signiert und verknüpfen eine Entität mit dem öffentlichen Schlüssel. Ein Kontaktnehmer kann über den öffentlichen Schlüssel aus dem Zertifikat die Identität prüfen, z.B. bei der Verifizierung einer Webseite. Digitale Signaturen werden verwendet, um Informationen auf ihre Vertrauenswürdigkeit zu prüfen. In einer public Key-Infrastruktur bildet die Verifizierbarkeit der Zertifikatsaussteller über sogenannte Stammzertifikate („Root Certificates“) das erste Glied in der Vertrauenskette.

Bei einer Vielzahl von Szenarien tragen auf Zertifikaten beruhende Sicherheitsmechanismen wesentlich zur Sicherheit bei:

[7] Noch einmal ausführlich erörtert in der Studie von ENISA. Information Security and Privacy Standards for SMSe 2015.

- Mails von Versicherungen können von der Empfängerin bzw. vom Empfänger überprüft und Phishing dadurch erschwert werden.

- Eine Internetverbindung vom Browser einer Nutzerin bzw. eines Nutzers zum Login seiner Bankverbindung kann sicherer gemacht werden.

- Postnachrichten von Nutzern können mittels digitaler Identität überprüft werden.

- Eine Vielzahl von Behördengängen (Steuererklärungen etc.) können anhand der digitalen Identitäten sicher elektronisch abgewickelt werden.

- Gesundheitsdienstleistungen und Zahlungen können anhand der digitalen Identität authentifiziert, signiert und verschlüsselt werden, z.B. können Laborresultate den Patienten verschlüsselt zugestellt werden, und diese können die Herkunft authentifizieren.

Aufgrund der Bedeutung von Vertrauen und Sicherheit im Netz sind Zertifikate bereits heute eines der wichtigsten Angriffsziele für Cyberangriffe. Gestohlene Zertifikate spielen bei einer Vielzahl von Angriffsmustern eine entscheidende Rolle. So waren etwa beim bekannten Stuxnet-Angriff auf die Uran-Anreicherungszentrifugen im Iran korrumpierte digitale Zertifikate ein Grundpfeiler, um die Sicherheitsmechanismen auszuhebeln.

In Zukunft werden Angriffe auf Zertifikate weiter zunehmen, da sie auch im IoT einen Grundpfeiler des Vertrauens bilden. Bei der Kommunikation zwischen Maschine und Mensch, aber auch zwischen zwei Maschinen (M2M) muss die Identität überprüfbar sein. Hier stellt sich das Problem, dass die Lebensdauer von digitalen Zertifikaten (oft zwei Jahre) deutlich kürzer ist als die der IoT-Geräte, insbesondere im B2B-Bereich mit über zehn Jahren. Der Herausforderung Zugangs- und Identitätsmanagement (IAM) bei der M2M-Kommunikation wird noch zu wenig Beachtung geschenkt.

Grundsätzlich ist ein sicheres Identitäts- und Zugangsmanagement („Identity and Access Management", IAM) bei jeder Organisation mit unter Umständen Tausenden von verschiedenen Zugriffsrechten für Menschen und vernetzte Geräte abhängig von einem von Grund auf vertrauenswürdigen Authentisierungs- und Informationsvalidierungssystem, das bei sichereren Systemen auf Zertifikaten beruht.

Nötig ist der Aufbau eines Netzwerks mit vertrauenswürdigen CA mit breiter Vereinbarkeit von Browsern und Betriebssystemen:

- Es ist sicherzustellen, dass juristische und natürliche Personen und Behörden in der Schweiz ein Zertifikat von einer vertrauenswürdigen Schweizer CA erhalten können.
- Alle sensitiven Entitäten (wie u.a. auch ein Web-Server) von Betreibern kritischer Infrastrukturen sowie von Identity Providern im Sinne des kommenden E-ID-Gesetzes sollen sich auf eine in der Schweiz aufgebaute und überprüfte bzw. überprüfbare public Key-Infrastruktur abstützen und nicht digitale Zertifikate aus dem Ausland verwenden.
- Privatpersonen sollen auf sicherem Weg eine digitale Identität erhalten, die vor Schadsoftware auf privaten Rechnern geschützt ist. Es sind Wiederherstellungsmechanismen bei Verlust und für Updates vorzusehen. Diese Wiederherstellung bedingt eine Identifikation der Person vor Ort (z.B. in einer Poststelle, einem Bahnhof oder allenfalls einer Bank).

- Es braucht wirksame Widerrufs- und Neuzertifizierungsmechanismen auf allen Ebenen im Falle von Verlust, Beschädigung oder Diebstahl eines privaten Schlüssels. Diese sind in das bestehende Ökosystem mit Betriebssystem (Mac OS, Windows, Unix, Android usw.) und Anwendungen (Browser, Email-Client usw.) zu integrieren.

Anonyme Anmeldenachweise („anonymous Credentials“) sind Token (Zugriffsinformation), die es einem Nutzer ermöglichen, Informationen über sich selbst und seine Beziehungen zu öffentlichen und privaten Organisationen anonym zu gestalten. Das System beruht auf kryptografischen Algorithmen. Dieser Ansatz ist datenschutzfreundlicher als die herkömmliche zentrale Verwaltung grosser Mengen von Benutzerdaten.

Personalisierte und nicht anonyme Anmeldenachweise in der analogen Welt sind Pässe, Führerscheine, Kreditkarten, Krankenversicherungskarten, Club-Mitgliedskarten etc. Diese enthalten den Namen des Eigentümers und weisen authentifizierende Informationen wie Unterschrift, PIN oder Foto auf, um zu verhindern, dass sie unrechtmässig verwendet werden. Anonyme Zugangsdaten in der analogen Welt sind Bargeld, Bus- und Bahntickets und Arcade-Spielmarken. Diese beinhalten keine identifizierenden Informationen und können deshalb zwischen den Nutzern übertragen werden, ohne dass die Aussteller oder Vertrauenspersonen davon Kenntnis haben. Identitäts- und Anmeldenachweise werden von Organisationen ausgestellt, welche die Authentizität der Informationen überprüfen und auf Anfrage verifizierenden Stellen übermitteln können.

Ein anonymer Nachweis macht bei einem digitalen Anmeldeverfahren so weit Aussagen über den Besitzer, dass ausreichend Informationen für die Erfüllung eines spezifischen Kriteriums vorliegen und die Berechtigung erteilt werden kann, aber ohne dass die ganze Identität des Benutzenden offengelegt wird. In gewissen Situationen ist dies von Vorteil und stärkt den Datenschutz. Dazu gehören etwa die Untergrenze für das Alter der Person, das Vorhandensein eines Führerscheins, in vielen Beziehungen die Staatsbürgerschaft oder Informationen darüber, ob noch offene Zahlungen des Gesuchstellers gegenüber einer bestimmen Organisation vorliegen.

IBM Research hat im Rahmen von europäischen Projekten wie Prime, PrimeLife und ABC4Trust diesen technischen Ansatz intensiv untersucht. Bisher hatten solche „anonymous Credentials“ aufgrund der fehlenden Umsetzbarkeit in der Praxis nur einen begrenzten praktischen Nutzen, mittlerweile haben sie aber einen Reifegrad erreicht, der eine konkrete Umsetzung ermöglichen würde. So hat eine gemeinnützige Stiftung, die Privacy by Design Foundation[8], den Ansatz weiterentwickelt und für die praktische Anwendung zur Verfügung gestellt.

[8] https://privacybydesign.foundation [Stand Juli 2018].

Empfehlungen:

5. Der Bund schafft die notwendigen gesetzlichen Grundlagen für sichere staatlich anerkannte digitale Identitäten (für juristische und natürliche Personen sowie digitale Infrastrukturen).
6. Der Bund prüft die Möglichkeit, soweit Identifizierungen nicht notwendig sind, anonyme Anmeldenachweise („anonymous Credentials“) einzuführen, insbesondere für die Beziehungen zwischen Privaten und Behörden, aber auch als Mittel für die Online-Nutzer.

4.5 Chancen für Lösungsansätze

4.5.1 Wie misst man Informationssicherheit?

Eine wichtige Frage für potentielle Lösungsansätze ist, wie man Informationssicherheit messen kann. Grundsätzlich hat die Informationssicherheit mit den Attributen Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit klare Kriterien aufgestellt. Gleichzeitig wurde in den letzten 20 Jahren eine Vielzahl von IKT- und Informationssicherheits-Standards, -Leitfaden, Checkbüchern usw. erarbeitet. Viele haben mittlerweile eine breite Anwendung gefunden und geholfen, die Sicherheit zu verbessern, indem Kontrollfragen (Controls) systematisch abgearbeitet werden. Indes fehlen im sich rasch ändernden technischen Umfeld nach wie vor die Erfahrungswerte, welche Schutzmassnahmen zu welchem Sicherheits- und Verwundbarkeitsniveau führen. Da die Bedrohung täglich ändert, nicht greifbar ist und die Wirksamkeit von Schutzmassnahmen entsprechend herabsetzt, kann weder von den Schutzmassnahmen noch von der Bedrohung eine Mess- und Vergleichsgrösse abgeleitet werden. Zusätzlich fehlt es an Vergleichsdaten.

Das Fehlen einer sicheren Messgrösse erschwert die Diskussion, welches Sicherheitsniveau für eine Organisation in ihrem spezifischen Kontext verhältnismässig ist und welche konkreten Schutzmassnahmen in welchem Kontext den grössten Sicherheitsgewinn erbringen. Eine moderne Gesellschaft in der digitalen Transformation braucht diese Messbarkeit oder zumindest Orientierungswerte, um dieses Risiko handhabbarer zu gestalten. Das Fehlen dieser Werte und einer entsprechenden Ereignishistorie erschwert auch die Versicherbarkeit dieser Risiken.

4.5.2 Nationales Netzwerk zur Förderung der Informationssicherheit

Die Schweizer Wirtschafts-, Forschungs- und Bildungslandschaft ist von Technologie und Innovation sowie vom Dienstleistungsgedanken geprägt. So gibt es eine Vielzahl von Stakeholdern, die sich intensiv mit der Informationssicherheit beschäftigen oder daran interessiert sind: im Finanz- und Versicherungssektor, in den Bereichen Gesundheit, Pharma, Verkehr, Energie, Informations- und Kommunikationstechnologien und auch bei einer Vielzahl von akademischen Einrichtungen. Koordination und der Austausch von Informationen (insbesondere über Vorfälle) finden jedoch kaum statt.

Gegenwärtig gibt es nur wenige und nicht miteinander verbundene Informationssicherheitsprojekte des Schweizerischen Nationalfonds (SNF). So gibt es mehrere Projekte im Rahmen des Nationalen Forschungsprogramms 75 (Big Data), die sich mit Informationssicherheit beschäftigen. Der Technologietransfer von der Wissenschaft in die Wirtschaft findet zwar statt, aber lediglich in der Form von Einzelprojekten und nicht in einer strukturierten Form. Start-ups und Entwicklungen im Sicherheitsbereich wie ID-Quantique, ProtonMail, Threema und Ethereum haben ihren Ursprung in der Schweiz

und deuten an, was möglich wäre; viel vom Potenzial liegt aber brach oder wird im Ausland umgesetzt.

Was fehlt, ist ein strukturiertes Ökosystem, ein „Hub“, wo landesweit Partner aus Wirtschaft, Wissenschaft und Staat eine langfristige Zusammenarbeit aufbauen können. Gelder aus Wirtschaft und Staat müssten dieses Ökosystem stützen – allenfalls im Rahmen eines grossen Innosuisse-Programms. Ein Ansatz ist die Schaffung eines Nationalen Netzwerkes, wo Unternehmen, Forschungseinrichtungen, Universitäten, Fachhochschulen und Start-ups Hand in Hand arbeiten und Wissen und Ressourcen bündeln. Der Aufbau von einem bis zwei nationalen Forschungszentren, sogenannten NCCR („National Competence Center in Research"), würde den Prozess unterstützen.

Aufgrund des Handlungsbedarfs in der Informationssicherheit sind verschiedene Staaten daran, mit bedeutenden Mitteln Forschungsinstitute auf- und auszubauen wie etwa Deutschland das Helmholtz Institut oder die Max-Plank-Gesellschaft. Die EU hat die Europäische Agentur für Netz- und Informationssicherheit (ENISA) aufgebaut. Solche Massnahmen werden ihre Wirkung nicht verfehlen, werfen aber auch Fragen bezüglich der Effektivität auf.

Das Beispiel Israels zeigt, wie ein vernetzter Ansatz mit einem Staatsprogramm von oben (National Cyber Bureau), der Einbindung aller Stakeholder in einem „Cyber-Spark“ und dem Aufbau eines „Cyberhub" (Ben Gurion Universität) ein einzigartiges und global erfolgreiches Ökosystem hervorgebracht hat. Ein solches Ökosystem würde in der Schweiz die Forschung und Entwicklung im Bereich Digitalisierung und Informationssicherheit nachhaltig fördern. Ebenfalls würde ein solcher Hub neue Studierende und Talente anziehen.

Empfehlungen:

7. Der Bund sorgt für die Schaffung eines nationalen Netzwerks zur Förderung der Forschung im Bereich der digitalen Transformation mit Schwerpunkt Informationssicherheit und des Wissenstransfers zwischen der Forschung und der Wirtschaft.

4.5.3 Fehlendes Lagebild und Wissensaustausch

In der physischen Welt führen die Polizei, die Nachrichtendienste und die Armee ein umfassendes Lagebild über Ereignisse und sich abzeichnende Risiken. Ein entsprechendes Lagebild der Cyberwelt mit einer umfassenden Quantifizierung fehlt. Ein Grund dafür ist die Globalität der Cyberbedrohungen, die sich an keine territorialen Grenzen halten; ein anderer, dass eine Mehrheit von Betroffenen Sicherheitsvorfälle nicht melden oder öffentlich machen, womit wichtiges Wissen nicht weitergegeben wird. Insbesondere in Europa überwiegt das „need to know“ Prinzip: die Weitergabe erfolgt nur, wenn es unabwendbar oder vorgeschrieben ist.

Während die Seite der Angreifer erkannt hat, dass Wissensaustausch und Aufgabenteilung massgeblich für den Erfolg ist, hat sich auf der Seite der Verteidigung diese Erkenntnis nur partiell durchgesetzt. Die verschiedenen privaten und staatlichen CERT („Computer Emergency Response Team"), die Informationssicherheitsunternehmen und nicht zuletzt die Vielzahl von betroffenen Unternehmen sammeln konstant Daten über Angriffe oder Hinweise durch Dritte, hingegen mangelt es an Zusammenarbeit und Wissensaustausch, um über ein fragmentiertes Lagebild hinauszukommen. Ein intensiver Wissensaustausch würde zu einer besseren Vorfallbewältigung beitragen (s. nachfolgende Ziff. 4.5.4). Diese Chance zur Zusammenarbeit muss durch Pro-

gramme und gegebenenfalls auch Regulierung genutzt werden. Die nötigen Instrumente werden im Rahmen des Akteurverhältnisses Staat-Gesellschaft (G2Ci/B) vertieft und entsprechende Empfehlungen formuliert (s. Ziff. 8.2.5).

4.5.4 Vorfallbewältigung (Incident Management)

Da es keinen vollständigen und abschliessenden Schutz gegen Cybervorfälle gibt, aber mit einer zunehmenden Anzahl gezielter Angriffe zu rechnen ist, ist der Aufbau und Betrieb einer landesweiten und zentralen Organisation zur Bewältigung von Vorfällen (Incident Management) ein Kernelement im Umgang mit Cyberrisiken. Zur Vorfallbewältigung gehört es, Vorfälle so früh wie möglich zu erkennen, die richtigen Gegenmassnahmen zu identifizieren und umzusetzen sowie die Vorfälle zu analysieren und daraus Erkenntnisse für die Verbesserung der Prävention abzuleiten. Um diese Aufgaben wahrzunehmen, braucht es Fachkompetenzen, Analyseinstrumente, eine gut funktionierende Organisation und eine intensive Zusammenarbeit zwischen allen relevanten Stellen. Entscheidend ist der Informationsaustausch auf einer breiten Basis gegenseitigen Vertrauens zwischen den Partnern. Dies ist umso wichtiger, da Angriffe oft verschiedene Stellen treffen und gemeinsam schneller und effektiver bewältigt werden können.

Ein engerer Kreis von Betreibern kritischer Infrastrukturen wird seit 2004 bei der Erkennung, Bewältigung und Analyse von Cybervorfällen durch MELANI (Melde- und Analysestelle Informationssicherung) unterstützt. MELANI funktioniert als Anlaufstelle auf staatlicher Ebene und bietet Unterstützung bei der technischen und nachrichtendienstlichen Analyse der Vorfälle und der dazugehörenden Informationsaustauschplattform. Anhand des Bedarfs nach einer zentralen und landesweiten Organisation und mit Blick auf die gesamtgesellschaftliche Dimension ergibt sich die Chance, die Zielgruppe von MELANI auszuweiten (s. Ziff. 8.2.5).

4.5.5 Informationssicherheit und Regulierung

Oft wird das Argument ins Feld geführt, dass die Wahl von Informationssicherheitsmassnahmen oder gar der Verzicht darauf jedem selbst überlassen werden muss. In der Folge würden letztlich die Marktmechanismen zu einem ausgewogenen IKT-Risikomanagement führen: Wer zu wenig in die IKT-Sicherheit investiert, verschwindet ebenso vom Markt wie das Unternehmen, das zu viel investiert und dem zu wenig Mittel für die Innovationsentwicklung bleiben. Dieser Ansatz des sich selbst regulierenden Marktes mag aus ökonomischer Sicht richtig sein, in der Cyberwelt geht er von falschen Voraussetzungen aus; denn fehlt ein adäquater Schutz, steigt das Risiko auch für andere. Die Angreifer missbrauchen ungeschützte Infrastrukturen als „Botnets" für Spam-Kampagnen, DDoS Angriffe, für ihre C&C Infrastruktur („Command and Control") oder deren Verschleierung. Schliesslich generieren erfolgreiche Ransomware-Angriffe und die Vermarktung von entwendeten Daten noch mehr Ressourcen für die Angriffsarsenale der Angreifer. Der libertäre reaktiv angelegte Ansatz mag letztlich nach einer Vielzahl von Schadensereignissen und Gegenmassnahmen auch zu einem Gleichgewicht zwischen Schutzlevel und Angriffspotenzial führen, dies aber zu weitaus höheren Bewältigungskosten und einer hohen Verunsicherung der Gesellschaft.

Eine Diskussion ist deshalb dringend nötig, wieviel Informationssicherheit verhältnismässig ist, wie die dafür notwendigen sicherheitstechnischen und organisatorischen Auflagen samt gesetzlicher Grundlagen aussehen, wer für deren Durchsetzung verantwortlich ist und in welchen Sektoren für welchen Sicherheitslevel es regulatorische Massnahmen braucht.

Im Unterschied zur EU oder auch den USA wurde diese Diskussion in der Schweiz noch nicht intensiv geführt. Es stellt sich die Frage, wieviel Informationssicherheit notwendig und verhältnismässig ist. Gleichzeitig zeigt sich die Gesellschaft zusehends fragil, mit Unsicherheiten umzugehen und Risiken in unbekannter Höhe zu akzeptieren. Ohne Antworten wird das Risiko „fehlende Informationssicherheit“ ein für die Gesellschaft nicht mehr tragbares Niveau erreichen, denn sie erwartet, dass auch das Cyberrisiko statistisch fassbar und beherrschbar wird. In diesem Zusammenhang hat die Expertengruppe die Bedeutung der Versicherbarkeit von Cyberrisiken für Wirtschaft und Gesellschaft erkannt, aber im Bericht nicht weiter ausgeführt.

Standards und Zertifizierung von Produkten und Dienstleistungen sind Teil dieser Diskussion, ebenso die Meldepflicht bei Cybervorfällen und der Bedarf bzw. die Festlegung respektive Regulierung von Schutzmassnahmen in der Informationssicherheit.

4.5.6 Neue Technologien: Künstliche Intelligenz-Mechanismen zur Verteidigung

Technische Sicherheitsmassnahmen wie etwa Virenscanner, Firewalls, Schnittstellen- und Applikationskontrollen funktionieren heute hauptsächlich nach vordefinierten Regeln. Dieser Ansatz gerät immer öfter an seine Grenzen: Einerseits nimmt die Anzahl von Varianten der immer selben Stämme von Schadsoftware zu, deren Erkennung die gängigen Systeme nicht sicherstellen können. Andererseits werden die digitalen Infrastrukturen immer komplexer und vernetzter, was die Einstellung von Hunderten oder Tausenden von Regeln, z.B. bei Firewalls, schlichtweg nicht mehr administrierbar macht; denn das Management der Regeln muss nicht nur aufgebaut, sondern ständig manuell und mit Hilfe von Expertinnen oder Experten gepflegt werden.

Grosse Hoffnungen werden deshalb in selbstlernende Systeme (Deep Learning) gesetzt. Diese interpretieren etwa bei der Einstellung eines Firewall-Regelwerks anhand der gewonnen Daten aus dem Datenverkehr die Eingangseinstellungen und passen diese bei Erweiterungen oder Aktualisierungen des Systems flexibel und automatisiert an. Weiter können solche Systeme bei der Überwachung von Applikationen Routinen (z.B. die Kommunikation mit anderen Systemen, Abweichungen bei der Bandbreite, Ports und Transportprotokolle) erkennen und unerlaubte Funktionen blockieren, da sie vom Standardverhalten abweichen oder Schwachpunkte bei der Programmierung aufdecken. Grundlage dafür ist die Mustererkennung, was eine Applikation tut und ob sie Ausgangspunkt für Anomalien beim Datenverkehr ist; dieser Ansatz wird schon breit verwendet. So vielversprechend die verschiedenen Ansätze sind, die dort, wo die Industrialisierung hinterherhinkt, automatisierte und intelligente Sicherheit in Aussicht stellen, so ist der Nutzen bis heute doch beschränkt. Die Herausforderung liegt darin, dass die selbstlernenden Systeme auf hochwertiges Daten- bzw. Trainingsmaterial angewiesen sind. Systeme im Betrieb könnten bereits korrumpiert sein und ein falsches Bild eines sicheren „Normalzustandes“ wiedergeben. Noch nicht angeschlossene neue Systeme hingegen vermitteln noch kein Bild des realen Betriebs. Die Folge ist, dass solche Systeme noch mehr falsche Alarme (sogenannte false Positives) melden, die Sicherheitsexpertinnen oder -experten wieder manuell überprüfen müssten, oder dass die Systeme eine Korrumpierung des Systems aufgrund des bereits korrumpierten Trainingsmaterial gar nicht erkennen. Zudem kann ein Angreifer potenziell die Trainingsphase von selbstlernenden Systemen beeinflussen, um fehlerhaftes Verhalten anzulernen, welches z.B. korrektes Verhalten als verdächtig einstuft, damit noch mehr falsche Alarme erzeugt werden.

Es ist zu befürchten, dass auch die Angreifer auf allen Ebenen (Kriminelle, staatsnahe Akteure, Nachrichtendienste, Militär und Polizei) angesichts der zunehmenden kostengünstigen Verfügbarkeit und Vereinfachung selbstlernende Systeme benutzen werden. Bereits heute setzen Angreifer die Technologie dafür ein, alltägliche Verhaltensmuster eines Netzwerks in einer Organisation zu analysieren. Die Ergebnisse verwenden sie dann dafür, Angriffsmuster zu entwerfen, die als Normalverhalten verschleiert werden. Ebenso lassen sich automatisiert personalisierte Phishing-Angriffe durchführen. Es ist davon auszugehen, dass das Wettrüsten zwischen Angreifern und Schützern auch hier zunehmen und die Cybersicherheit zukünftig prägen wird. Umso mehr ist es nötig, dass die Forschung hier intensiviert wird. Der Staat, kritische Infrastrukturen, Forschungsstellen und nicht zuletzt auch die sensitive Industrie müssen für diesen Wettlauf gerüstet sein (s. auch Ziff. 8.2.6f).

5 Analysefeld Business to Consumer (B2C)

5.1 Ist-Zustand und weitere Entwicklung

Die Digitalisierung hat zu einer Vielfalt neuer kostengünstiger Angebote zugunsten der Benutzer und Verbraucher von bisher mehrheitlich elektronischen Güter- und Dienstleistungslieferungen geführt. Die Dienstleistungen sind individualisierbar, auf den Kundenbedarf zugeschnitten, überall und rund um die Uhr erhältlich. Es ist davon auszugehen, dass die Angebotsvielfalt weiter zunehmen wird. In dem Masse, wie sich die Grenzen zwischen der virtuellen digitalen und der physischen Welt auflösen, werden auch die Dienstleistungen diese Grenze nicht mehr kennen. Der digitale Sekretär, der für seinen Dienstherren via Drohnenservice einen neuen Regenschirm bestellt, weil er aufgrund der Videoüberwachung weiss, dass sein Dienstherr seinen alten auf dem Arbeitsweg liegengelassen hat, liegt viel näher bei der Realität als bei einer Science Fiction-Erzählung.

Die heute dominierenden Internet-Unternehmen (Google, Apple, Facebook, Amazon, Alipay/Alibaba etc.) kontrollieren in ihrer Position als „Gatekeeper“ die Zugänge zum sichtbaren Teil des Ökosystems Internet. Dadurch haben sie eine monopolartige Stellung bei den Dienstleistungen Suchmaschine, Soziale Plattform und Online-Shopping und - in einem noch geringen Ausmass – bei den Clouddienstleistungen erreicht. Viele Detailhändler haben im Onlinegeschäft ihren Platz in der Wertschöpfungskette Richtung Konsumenten abtreten müssen oder sie können nur noch via Kooperation mit den Gatekeepern erfolgreich sein. Im weiteren Verdrängungskampf bei der Kontrolle über die Schnittstelle zwischen digitalem Service und Menschen könnte die Sprachsteuerung eine wesentliche Rolle spielen und der Treiber für weitere Zentralisierungseffekte sein; denn warum soll sich ein zukünftiger Anwender mit verschiedenen sprachgesteuerten Schnittstellen abmühen, wenn er alles mit einem digitalen Sekretär abwickeln kann? So erstaunt es nicht, dass sich die grossen Internetanbieter bereits mit Sprachassistenten (Amazon mit Alexa, Google mit Google Now, Apple mit Siri und Microsoft mit Cortana) in Stellung gebracht haben.

Die Anbieter statten ihre digitalen Dienstleistungen zunehmend mit künstlicher Intelligenz aus. So ist es vorstellbar, dass künftig mächtige Applikationen mit den Kapazitäten des heutigen IBM Watson den Kunden zur Verfügung stehen. Die erwähnten Sprachassistenten stellen nur den ersten Schritt zu einer anthropomorphen Gestaltung dieser Applikationen dar. Wie in der analogen Welt steigt der Wert dieser personalisierten Applikationen in dem Mass, wie sie ihren Arbeitgeber und dessen Routinen, Präferenzen und Vergangenheit kennen.

Insbesondere bei den sozialen Netzwerken gibt es einen Widerspruch bei den Nutzerinnen und Nutzern. Einerseits geben diese immer mehr personenbezogene Daten (Name, Bilder, Mobile-Nummer, sogar religiöse Bekenntnisse) im Netz preis, andererseits ist ihnen der Schutz ihrer Privatsphäre wichtig. Eine Mehrheit scheint jedoch bei der Güterabwägung die Teilhabe am sozialen Leben im Netz klar zu priorisieren. Da aber gerade soziale Netzwerken die Preisgabe von persönlichen Daten voraussetzen, stellen das Verhalten des Nutzers und das Geschäftsmodell des Anbieters ein Dilemma für den Daten- und Konsumentenschutz dar.

Die digitale Transformation verändert im Bereich „Business to Consumer“ grundlegend das Verhältnis zwischen Anbietern und Nutzern. Neben den allgemeinen Merkmalen der Digitalisierung (etwa der ständigen Verfügbarkeit von Informationen) sind Big Data Analysen respektive selbstlernende Systeme, datengetriebene Geschäftsmodelle –

insbesondere die Herausgabe personenbezogener Daten gegen „Gratis“- Dienstleistungen – und zweiseitige Märkte die zentralen Treiber für die Entwicklung im B2C-Bereich. Obwohl viele digitale B2C-Dienstleistungen zwei bzw. alle drei Elemente beinhalten, sind die Auswirkungen gesondert zu betrachten.

5.2 Chancen und Risiken

Big Data Analysen sind dort massgebend, wo Anbieter mittels Kundentracking und Datenanalyse Persönlichkeitskprofile (Profiling) und Wertungen (Scoring) von Nutzerinnen und Nutzern bzw. Nutzergruppen erstellen. Beim Scoring werden personenbezogene Daten auf einen Wert zusammengezogen, womit der Vergleich zwischen Menschen vereinfacht wird. Das Profiling strebt hingegen danach, anhand einer automatisierten Auswertung personenbezogener Daten möglichst viele Fragen zu einer identifizierbaren Person zu beantworten und dadurch eine hohe Personalisierung zu erreichen. Noch nie zuvor hatte der Anbieter von Produkten und Dienstleistungen so viele Informationen über jeden einzelnen Nutzer, wie wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Verhalten, Aufenthaltsort usw.

Diese Informationsdichte ermöglicht einerseits einen hohen kundenorientierten Komfort und Service. Andererseits können diese Informationen zu einer Diskriminierung von Personen oder Personengruppen führen. Profiling und Scoring können für den Nutzer insbesondere in den Bereichen Kreditwürdigkeit, Versicherungswesen, Analyse von Bewerbungen, neutrale Informationsvermittlung, Beurteilung des Personals im HR-Bereich und – vorderhand noch weniger ausgeprägt – beim Zugang zu Ausbildungsmöglichkeiten negative Konsequenzen nach sich ziehen: Zum Beispiel erhält der Nutzer keinen Zugang zum Produkt oder nur zu überhöhten, nicht transparent dargelegten Preisen, oder er wird bei Bewerbungsverfahren aus unbekannten Gründen ausgeschlossen oder gar nicht berücksichtigt. Ebenfalls ist denkbar, dass in Zukunft soziale Netzwerke Nutzer aufgrund von Scorings ausschliessen.

Das Profiling ermöglicht auch sogenannte „positive Filterblasen“. Dies bedeutet, dass der Suchassistent tatsächlich die Informationen priorisiert, bei denen er von einem Mehrwert für den Nutzer bezüglich Inhalt und Relevanz ausgehen kann - eine Überprüfung der Glaubwürdigkeit der angezeigten Informationen wäre zwar wünschenswert, aber aufgrund des Technikstands ein langfristiges Ziel. Obwohl auch positive Filterblasen sich vom Ideal eines neutralen Suchergebnisses entfernen, profitiert der Nutzer, denn die Reduktion der Informationsflut stellt einen wichtigen Service dar.

Weit mehr sind in der letzten Zeit „negative Filterblasen“ in die Schlagzeilen geraten. Bei negativen Filterblasen erhält der Nutzer die Ergebnisse, die ohnehin seinen Kenntnissen und Präferenzen entsprechen und keinen Wissenszuwachs mit sich bringen. Mit personalisierten negativen Filterblasen lassen sich Nutzer auch manipulieren, indem ihnen gewisse Informationen vorenthalten und/oder andere Informationen jenseits der normalen Suchgewichtung eingeblendet werden. So ist es möglich, dass einem Nutzer wesentliche Vergleichsinformationen oder alternative Informationen nicht mehr oder nur mit Mehraufwand (neue Suche und weites nach unten Scrollen, andere Suchmaschinen, legendierte Suche) zur Verfügung stehen. Das Fehlen komplementärer und substituierender Informationen kann den Nutzer schädigen. Wesentlich ist die fehlende Transparenz, wie das System zum Suchergebnis kommt. Während bei Medienseiten und sozialen Netzwerken davon ausgegangen werden muss, dass sie Suchergebnisse tatsächlich personalisieren, sind bei den Suchmaschinen trotz aller Gerüchte bis anhin nur positive Filterblasen bekannt.

Das Geschäftsmodell „Dienstleistung gegen personenbezogene Daten“ bei Suchmaschinen, sozialen Netzwerken, Gesundheitsdiensten (Trackern) oder Cloud-Massenspeicherlösungen hat sich weithin durchgesetzt und die Diskussion ausgelöst, wie in Zukunft mit der Wertigkeit von Daten verfahren werden soll (s. Ziff. 7.2).

Bei zweiseitigen Märkten spielen indirekte und direkte Netzwerkeffekte eine wesentliche Rolle: Je mehr Informationen Anbieter und Interessenten voneinander haben, desto effizienter funktioniert die Vermittlung von Diensten und Produkten. Preis, Auswahl und Bequemlichkeit werden für die Nutzer besser; die Anbieter wiederum erzielen mehr Umsatz. Aber auch die Risiken nehmen zu: Die Menge an personenbezogenen Daten, welche die Betreiber abgreifen, können zu einer Verletzung der Privatsphäre oder zu konsumentenschutzrechtlichen Missbräuchen führen.

Dazu gehört etwa die Preisdifferenzierung: Der Erfolg der Onlineshopping-Plattformen, das Tracking der Kundinnen und Kunden, die Analyse der Kundenprofile und die Automatisierung der Plattformprozesse ermöglichen hochflexible Preisbildungsmechanismen. Diese orientieren sich nicht nur an der allgemeinen Nachfrage und am Angebot und/oder an der Kaufkraft und dem Kaufverhalten eines Kundenkreises, z.B. Studierenden, denen ein einheitlicher Preis angeboten wird. Die moderne Datenbearbeitung und die Datendichte ermöglichen eine im ökonomischen Sinn perfekte Preisdifferenzierung.

Ein bekanntes Beispiel ist die Erhöhung des Preises für ein Flugticket nach jedem Klick, wenn der Konsument mehrmals den Preis eines Flugtickets konsultiert und der höhere Preis sich nicht durch Nachfragedruck rechtfertigen lässt. Positiv gesehen bringt die perfekte Preisdifferenzierung nicht nur Vorteile für den Anbieter, sondern auch für die verschiedenen Kunden. Wenn deren individuelle Zahlungsbereitschaft aufgrund des Mengen-Angebots-Verhältnisses und der Produktionskosten durch das Profiling bedient werden kann, profitieren Anbieter und Kunden gleichermassen. Negativ kann sich die perfekte Preisdifferenzierung auswirken, wenn die Preisunterschiede zu gross sind, sich schnell verändern, für Kunden nicht mehr nachvollziehbar und transparent sind, die Möglichkeit des Preisvergleichs wegbricht und Angebotsmonopole dem Kunden keine Ausweichmöglichkeiten geben.

Kritiker der digitalen Transformation im Bereich B2C stellen oft eine Wissensasymmetrie zugunsten des Anbieters fest. Dies ist zu kurzgefasst. Die Digitalisierung kann auch zu einer Stärkung der Konsumentenseite führen. Die Bewertungs- und Preisvergleichsportale zeigen die Angebotsvielfalt und die Preisvorteile. Damit wird auch der Anbieter zunehmend gläsern, obwohl dies aufgrund komplexer Angebote nicht in allen Sektoren wie etwa bei den Dienstleistungen (u.a. Versicherungsbranche) der Fall ist. Weiter kann der Konsument heute dank neuer technologischer Möglichkeiten selber eine Anbieterrolle übernehmen, und zwar als sogenannter „Prosument“. Bekannte Beispiele dafür sind die Beherbergungsplattformen: Der Mieter ist zwar gegenüber dem Vermieter der „schwächere Konsument“, hat aber gleichzeitig die Möglichkeit, seine Wohnung durch Untervermietung an Touristen zu kommerzialisieren.

Fazit
Risiken beim Schutz der Privatsphäre und der informationellen Selbstbestimmung und beim Konsumentenschutz sind nicht zu übersehen. Mit Blick auf die Diskussion des rechtlichen Handlungsrahmens und des Handlungsbedarfs spielen somit das Datenschutzrecht und Aspekte des Konsumentenschutzes eine wichtige Rolle. Spezifische Aspekte der Ethik werden in Ziffer 11 erörtert.

Risiken aus Sicht des Datenschutzes sind insbesondere zu orten:

- wenn die digitale Beobachtung der Nutzer (Tracking) und die maschinelle Datenbearbeitung bzw. die eingesetzten Algorithmen das Transparenzprinzip verletzen. Die Datenbearbeitung greift ohne das Wissen der betroffenen Personen in deren Privatsphäre und die informationelle Selbstbestimmung ein. Nachgelagert kann die betroffene Person weitere Schäden als Kunde und Nutzer erleiden.
- wenn die fehlende Transparenz der den Online-Angeboten zugrunde liegenden Datenbearbeitungen die Geltendmachung aller weiteren Rechtsbehelfe wie Einwilligungs-, Auskunfts- oder Widerspruchsrechte erschwert.
- wenn echte Wahlmöglichkeiten und Alternativangebote fehlen, was vor allem bei Monopolsituationen oder ungenügenden Ausweichmöglichkeiten der Fall sein kann - etwa bei sozialen Netzwerken, bei denen der Nutzer über seinen Online-Freundeskreis an die Plattform gebunden ist.

Mit Blick auf den Konsumentenschutz sind folgende Risiken festzuhalten:

- Die Digitalisierung ermöglicht neue digitale Vertragsinhalte und digitale Vertragsvereinbarungen, welche dazu führen können, dass die Transparenz und Durchsetzbarkeit der vertraglichen Rechte und Pflichten zum Nachteil der Konsumenten abnimmt (s. Ziff. 5.3.2.2 - Ziff. 5.3.2.4).
- Marktmächtige Stellungen und Profiling können zu einer Übervorteilung von Konsumenten führen (s. Ziff. 5.3.2.5).
- Der Gegenstand der digitalen Leistung und die Komplexität der digitalen Produktionsketten sind zu wenig geklärt, um Fragen der Haftung bzw. der Produktehaftung sachgerecht zu regeln (s. Ziff. 7.3).

5.3 Rechtlicher Ordnungsrahmen und Handlungsbedarf

Zwei Rechtsfelder verdienen im Analysefeld B2C besondere Beachtung: der Datenschutz und der Konsumentenschutz.

5.3.1 Schutz der Privatsphäre und der informationellen Selbstbestimmung

5.3.1.1 Einführung

Im Aktionsfeld B2C kommt dem Datenschutz eine zentrale Rolle zu, da dem Einzelnen gegenüber der Wirtschaft ein grundrechtlicher Anspruch auf Schutz der Privatsphäre und der informationellen Selbstbestimmung eingeräumt wird. Der Einzelne muss der Offenlegung der eigenen Persönlichkeit durch die Wirtschaft Grenzen setzen können, indem er über das Erheben, das Speichern und die Weitergabe seiner Daten selbst entscheidet. Die Diskussion, welche Vor- und Nachteile ein Eigentum an Daten mit sich brächte, und die Frage nach dem Zugang zu den eigenen Daten (Datenportabilität) werden als B2B und B2C übergreifende Themen separat behandelt (s. Ziff. 7).

5.3.1.2 Verhalten der Nutzerinnen und Nutzer

Die Zukunft des Datenschutzes hängt nicht nur von den technischen und rechtspolitischen Vorgaben im Datenschutzbereich ab, sondern auch davon, ob der europäische Konsument und Nutzer selber bereit ist, im konkreten Alltag den zeitlichen und intel-

lektuellen Aufwand zu leisten, um seine informationelle Selbstbestimmung aktiv wahrzunehmen. Umfragen zeigen, dass die Gesellschaft dem Datenschutz eine grosse Bedeutung beimisst, die Privatsphäre aber auch aufgrund des sogenannten Privacy Paradox und mangelnder Alternativen nicht überall und immer priorisiert wird. Schliesslich sind die Aufsichtsbehörden im Datenschutz auf die Hinweise einer datenschutzsensibilisierten Bevölkerung angewiesen, wenn es darum geht, datenschutzwidriges Verhalten aufzudecken und zu sanktionieren.

5.3.1.3 Ungenügende Harmonisierung des Datenschutzrechts auf globaler Ebene und Durchsetzbarkeit europäischer Datenschutzvorstellungen

Zum Datenschutz gibt es global gesehen unterschiedliche Vorstellungen, wie beispielsweise die Ungültigerklärung des Safe Harbor Abkommens EU-USA durch den Europäischen Gerichtshof, das lange Seilziehen mit den USA um das Nachfolgeprodukt „Privacy Shield“ und die Gerichtsfälle in Europa gegen die tonangebenden USA-Daten-Giganten zeigen.

Gleichzeitig lassen sich auf internationaler Ebene aber auch Harmonisierungsbestrebungen im Bereich des Datenschutzrechts feststellen. So ist die aktuelle Datenschutz-Konvention 108 des Europarates vom 28. Januar 1981 nicht nur von 47 Mitgliedstaaten des Europarates, sondern auch von Uruguay, Tunesien, Mauritius und Senegal ratifiziert worden. Weitere Staaten ausserhalb Europas, namentlich Marokko, Kapverden, Burkina Faso, Argentinien und Mexiko, sind im Begriff, das Übereinkommen zu ratifizieren. Das Interesse aussereuropäischer Staaten an einer Ratifizierung der Datenschutz-Konvention 108 könnte ausserdem weiter zunehmen, weil die Europäische Union dieses Interesse als wichtiges Kriterium für einen Angemessenheitsbeschluss (und damit für einen grenzüberschreitenden Datenverkehr ohne zusätzliche Schutzmassnahmen) betrachtet. Über einen solchen Angemessenheitsbeschluss, welcher ein Datenschutzniveau voraussetzt, das der Sache nach demjenigen der EU gleichwertig ist, verfügen neben der Schweiz derzeit auch Andorra, Argentinien, die Färöer Inseln, Guernsey, Israel, die Isle of Man, Jersey, Neuseeland und Uruguay. Weitere Drittstaaten wie Japan und Südkorea sind mit der EU für einen Angemessenheitsbeschluss im Gespräch.

Trotz dieser positiven Entwicklung für den europäischen Datenschutz drängt sich die Frage auf, ob sich angesichts der digitalen Übermacht aus dem aussereuropäischen Raum – insbesondere aus den USA und China - die europäischen Grundsätze des Datenschutzes durchsetzen lassen: Acht der zehn weltgrössten Unternehmen sind im digitalen Markt tätig und haben ihren Sitz in den USA oder in China.

5.3.1.4 Laufende Datenschutzrevision

Am 15. September 2017 hat der Bundesrat seinen Entwurf zur Totalrevision des DSG (E-DSG) verabschiedet und dem Parlament unterbreitet. Mit dem E-DSG soll der Datenschutz gestärkt und an die Realität der digitalen Datenbearbeitung angepasst werden. Gleichzeitig will der Bundesrat sicherstellen, dass die Schweiz über einen international anerkannten Datenschutz-Standard verfügt, der insbesondere die jüngsten Entwicklungen in Europa (DSGVO, Revision der Datenschutz-Konvention 108 des Europarates) berücksichtigt.

Während die bis anhin geltenden datenschutzrechtlichen Grundsätze wie die Rechtmässigkeit, die Verhältnismässigkeit, die Zweckbindung, die Erkennbarkeit und die Richtigkeit der Bearbeitung bekräftigt und mit Blick auf die Digitalisierung konkretisiert

werden, sieht der E-DSG auch neue Massnahmen vor, um das Datenschutzrecht an die technologischen Entwicklungen anzupassen. Dazu gehören insbesondere:

- die Erhöhung der Transparenz durch eine Erweiterung der Informationspflicht bei der Beschaffung von Personendaten und durch die Einführung einer Meldepflicht gegenüber der Datenschutzaufsicht bei Verletzungen der Informationssicherheit.
- die Konzepte des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen ("Privacy by Design and by Default"): Die Grundidee hinter diesen Konzepten ist, dass organisatorische und technische Vorkehrungen die Gefahr von Verstössen gegen das Datenschutzrecht erheblich mindern können. Die Verantwortlichen werden deshalb verpflichtet, ihre Datenbearbeitungen von Anfang an organisatorisch und technisch so zu gestalten, dass die Datenschutzvorschriften eingehalten und so wenig Daten wie möglich bearbeitet werden. Ausserdem müssen die Voreinstellungen einer Datenbearbeitung standardmässig möglichst datenschutzfreundlich eingerichtet sein.
- die Datenschutz-Folgenabschätzung: Mit diesem in der digitalen Praxis bewährten Instrument müssen die Verantwortlichen hohe Risiken ihrer Datenbearbeitungen frühzeitig dokumentieren und gegebenenfalls angemessene Schutzmassnahmen treffen. Je nach Ergebnis muss der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) konsultiert werden, welcher zusätzliche Massnahmen vorschlagen kann, um die festgestellten Risiken einzudämmen.
- neue Vorschriften betreffend Profiling und automatisierte Einzelentscheidungen: Diese beiden Datenbearbeitungsformen haben im Zeitalter von Big Data an Bedeutung gewonnen. Sie sind grundsätzlich zulässig, werden aufgrund ihres Risikos für die Persönlichkeitsrechte aber strengeren Anforderungen unterworfen als andere Bearbeitungsformen.
- die Stärkung der Datenschutzaufsicht, indem dem EDÖB statt Empfehlungs- neu Verfügungskompetenzen eingeräumt werden.
- strengere Strafbestimmungen: Einerseits hat der Bundesrat die im DSG enthaltenen Straftatbestände erweitert. Andererseits hat er die bisherige Bussenobergrenze von Fr. 10 000.- auf 250 000.- angehoben.

Mit diesen und weiteren Massnahmen sieht der E-DSG die erforderlichen Bestimmungen vor, um das schweizerische Datenschutzrecht unter anderem der DSGVO anzunähern und um die Ende Mai 2018 verabschiedete revidierte Datenschutz-Konvention 108 des Europarates zu übernehmen. Anders als die DSGVO sieht der E-DSG aber etwa kein Recht auf Datenportabilität vor. Auch das vorgeschlagene Sanktionssystem hebt sich von der DSGVO deutlich ab: Zum einen fallen die Bussen deutlich tiefer aus, und zum anderen sieht der E-DSG keine Verwaltungssanktionen vor. Der Bundesrat zieht vielmehr das bestehende System vor, sodass die ordentlichen Strafgerichte für die Sanktionen zuständig bleiben. Schliesslich enthält der E-DSG im Unterschied zur DSGVO kein eigentliches Koppelungsverbot. Dieses verbietet es, den Abschluss eines Vertrages an die Einwilligung in die Bearbeitung von Daten zu knüpfen, die für die Erfüllung des Vertrags nicht notwendig sind. Der E-DSG ist derzeit im Parlament hängig.

Viele der Massnahmen im E-DSG stellen keine grundsätzlich neuen Methoden dar. Massnahmen wie etwa die Risikofolgenabschätzung oder das Prinzip des „Privacy by Default“ gelangen heute in allen bedeutenden digitalen Datenbearbeitungsprojekten zur Anwendung. Insofern werden mit der Revision Elemente der guten Praxis in eine formell-gesetzliche Form überführt und Lücken geschlossen.

Die Massnahmen der guten Praxis sollen fortgeführt und intensiviert werden. Wesentlich für deren erfolgreiche Umsetzung sind auch die Datenschutzaufsichtsbehörden: Sie beobachten, ob und wie sich etwa datenschutzfreundliche Technologien trotz mangelnder globaler Harmonisierung im Datenschutzrecht in der Praxis durchsetzen, und wirken darauf hin, dass sich z.B. die benutzerfreundliche Verlinkung relevanter Passagen von AGB allmählich als Standard durchgesetzt.

Die Datenschutzaufsichtsbehörde des Bundes muss den Bedürfnissen der Gesellschaft und der Wirtschaft gerecht werden, indem sie die Begleitung digitaler Grossprojekte durch eine Kombination von Beratung und Aufsicht sicherstellt. Trotz Zunahme von digitalen Grossprojekten und der wachsenden Nachfrage nach Beratungsleistungen muss der EDÖB eine glaubwürdige Kompetenz aufbauen und ausreichende Kontrolldichte gewährleisten.

5.3.1.5 Herausforderungen bei der Revision des Datenschutzes und der künftigen Umsetzung

Der E-DSG hat unter anderem zum Ziel, das schweizerische Datenschutzrecht so weit als nötig an die DSGVO anzunähern, um den Angemessenheitsbeschluss der EU, welcher der Schweiz ein im Wesentlichen gleichwertiges Datenschutzniveau attestiert, beizubehalten. Ein Widerruf des Angemessenheitsbeschlusses hätte für die Schweiz im Wirtschaftsverkehr mit den EU-Staaten erhebliche Nachteile, da die Bekanntgabe von Personendaten aus der EU in die Schweiz nur noch möglich wäre, wenn zusätzliche Schutzgarantien abgegeben würden oder wenn bestimmte Ausnahmen erfüllt wären.

Seit Inkrafttreten der DSGVO bestehen bezüglich der administrativen Pflichten und Kompetenzen der personell ausgebauten und mit Verfügungskompetenzen ausgestatteten Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten und den Datenschutzbehörden in der Schweiz augenscheinliche Unterschiede. Ein für die Schweiz nicht anwendbares Prinzip der DSGVO besteht darin, dass beim grenzüberschreitenden Datenverkehr die Aufsichtsbehörde des jeweiligen EU-Mitgliedstaates alleinige Ansprechbehörde für die heimischen Unternehmen ist (One Stop Shop). Vor diesem Hintergrund ist es wichtig, dass schnell Rechtssicherheit geschaffen wird, indem die Schweiz die Totalrevision ihres Datenschutzrechts baldmöglichst abschliesst und mit der EU Verhandlungen über die Abgrenzung der territorialen Zuständigkeiten und die Zusammenarbeit der Datenschutzaufsichtsbehörden aufnimmt.

Die im E-DSG neu geregelten Datenschutzgrundsätze – etwa die Zweckbindung oder die Risikofolgenabschätzung – werfen Fragen auf, wie eine korrekte bzw. ausreichende Umsetzung auszusehen hat. So schreibt „Privacy by Default“ etwa vor, dass die Grundeinstellung datenschutzfreundlich zu gestalten ist, damit die Privatsphäre der betroffenen Person respektiert wird. Es dürfen nur die Daten erhoben werden, die für den Bearbeitungsprozess oder die Funktionsweise unabdingbar sind. Dies stützt auch das Prinzip der Datenminimierung. Was auf den ersten Blick abstrakt, einfach und zielführend klingt, ist in der Praxis oft schwierig, da die Trennlinie zwischen Haupt- und Nebenfunktionen einer Dienstleistung nicht immer klar ist – schliesslich hängen die Qualität und die Breite der Funktionalität oftmals direkt von der Datendichte über einen Nutzer ab. Die Datendichte setzt sich aus der Datenkategorie (Geschlecht, Alter, Positionsdaten etc.), der Aufbewahrungszeit und letztlich aus der permanenten Erfassung aller Datenpunkte ab. Lassen sich für eine spezifische Funktionalität die dafür minimal notwendigen Datenkategorien noch klar definieren (z.B. nur das Alter aber nicht das Geschlecht), kann sich die Definition des minimalen Datenbedarfs bei der

Aufbewahrungszeit und der lückenlosen Erfassung als zunehmend schwierig erweisen. Die Servicequalität beispielsweise bei einem Gesundheits-Tracker hängt von der lückenlosen Erfassung aller Daten ab. Nichtsdestoweniger muss die Transparenz gegenüber dem Nutzer gewahrt bleiben. Angesichts dieser anspruchsvollen Fragestellung ist wichtig, dass die Erarbeitung neuer digitaler Geschäftsmodelle und deren Infrastrukturen durch den unternehmensinternen Datenschutz begleitet wird.

Viele Unklarheiten werden erst durch aufsichtsbehördliche und justizielle Klärung von Präzedenzfällen ausgeräumt werden. Der Rechtsweg ist üblich und zielführend, kann aber langwierig sein. Bis zum Ergehen eines rechtskräftigen Entscheids bleiben die betroffenen Unternehmen im Unklaren, ob ihre Datenbearbeitungen Bestand haben. Im Sinne einer Orientierung dürfte hierbei auch der Blick in den EU-Rechtsraum wichtig werden. Dort zeichnet sich ein weitgehend einheitliches Datenschutzniveau ab, weil die DSGVO den nationalen Gesetzgebern nur noch geringen Spielraum lässt.

Die Expertengruppe erachtet das Risiko für erheblich, dass das revidierte Datenschutzrecht angesichts fehlenden Wissens bei Betroffenen und der beschränkten Kontrollressourcen der Datenschutzbehörden nicht die erhoffte Schutzwirkung entfalten kann und eine Kluft zwischen dem datenschutzrechtlichen Anspruch und der digitalen Realität zurücklässt. Allerdings zeigt die DSGVO, dass hohe Sanktionen Datenbearbeiter und betroffene Personen dazu veranlassen, sich viel intensiver mit dem Datenschutz zu befassen.

5.3.1.6 Big Data Analysen: Herausforderungen für den Datenschutz

Big Data Analysen zielen darauf ab, Daten aufzubereiten und zu verfeinern, um das Verhalten und den Zustand von Personen und Nutzergruppen zu erfassen. Der technische Fortschritt ermöglicht es, unstrukturierte Daten wie E-Mails, Audio- und Visio-Daten sowie digitale Dokumente schnell und differenziert auszuwerten; gleichzeitig erschwert er es, der rechtlichen Kategorisierung in personen- und nicht personenbezogene Daten gerecht zu werden. Die Arbeit mit anonymisierten Personendaten und mit Sachdaten, die ohne übermässigen Aufwand eine Zuordnung, Personalisierung oder Re-Identifizierung ermöglichen, machen Big Data zu einer zunehmenden Herausforderung für den Datenschutz.

Gelingt es, den Bezug zwischen Daten und Personen durch Anonymisierung oder rechtlich hinreichende Pseudonymisierung zu unterbrechen, liegen Sachdaten vor, deren Bearbeitung solange von der Datenschutzgesetzgebung ausgenommen bleibt, als dieser Bezug nicht wiederhergestellt wird. Bei der Anonymisierung geht es darum, die Verknüpfung zwischen differenzierenden Informationen und Personen durch Randomisierung oder Generalisierung zu trennen. Neuere Forschungsarbeiten (z.B. zur K-Anonymität, L-Diversität oder „differential Privacy") und Erfahrungswerte zeigen aber, dass die Anonymisierung eines Datenbestandes oft nur dann irreversibel ist, wenn der Informationsgehalt weitgehend entfernt wird. Deshalb ist zu erwarten, dass die aktuellen Anonymisierungstechniken sich immer weniger als hinreichend erweisen werden und neue technische Standards definiert werden müssen, um den Persönlichkeitsschutz zu gewährleisten. Mit der Anwendung von K-Anonymität, L-Diversität oder „differential Privacy" gehen aber zunehmend spezifische Informationen verloren. Bei der „differential Privacy" sind dann aufgrund des hinzugesetzten Datenrauschens nur noch statistische Auswertungen möglich. Dieser Sicherheitsanspruch führt dazu, dass wertschöpfende Analysen im Bereich Profiling nur noch bedingt möglich sind.

Die fortschreitende Technik und die Menge an vorliegenden Kontextdaten erlauben eine Re-Identifizierung, wenn die Daten nicht unumkehrbar anonymisiert sind. Eine vollständige Anonymisierung vermag aber unter Umständen das Potential von Big

Data Analysen einzuschränken; aus diesem Grunde muss den Risikofolgenabschätzungen beim Einsatz solcher Analysen ein grosses Gewicht zukommen.

Anonymisierte Personendaten fallen zwar nicht unter das DSG. Über die Beschaffung von reidentifizierten Daten muss der Datenbearbeiter aber gemäss E-DSG die betroffenen Personen nachträglich informieren (s. Art. 17 E-DSG). Diese Pflicht entfällt gemäss Art. 18 Abs. 2 E-DSG, wenn dies nicht möglich (lit. a) oder der Aufwand unverhältnismässig ist (lit. b). Insbesondere wird der Fall genannt, wenn eine sehr grosse Anzahl von Personen betroffen ist und der Aufwand für die Information mit einem unverhältnismässigen Aufwand verbunden ist. Allerdings führt die Botschaft zum E-DSG einschränkend aus, dass diese Ausnahme eng auszulegen sei. Der für die Datenbearbeitung Verantwortliche hat grundsätzlich sämtliche Vorkehren zu treffen, die unter den gegebenen Umständen von ihm erwartet werden können, um der Informationspflicht nachzukommen. Dadurch steigt für den Datenbearbeiter bei unklarem Informationsgewinn und unbekannter wirtschaftlicher Verwertbarkeit der Daten der Aufwand in einem nicht absehbaren Ausmass an. Das folgende Beispiel soll dies illustrieren. So ist es denkbar, dass ein Datenbearbeiter ausgewertete Genome mit einem klaren genetischen Fingerabdruck für eine weitere Bearbeitung mit neuem Zweck übernimmt, diese Datenliste aber keine Identitäts- und Kontaktdaten der betroffenen Personen beinhaltet. Die Pflicht des Datenbearbeiters, die Personen zu informieren, gestaltet sich entsprechend schwierig.

Weiter bleibt zu beachten, dass angesichts des datenschutzrechtlichen Zweckbindungsgebots eine Einwilligung des Betroffenen einzuholen ist, wenn die Datenbearbeitung im Rahmen von Big Data Analysen zu einer Zweckänderung führt (was oft der Fall sein dürfte). Die transparente Bezeichnung eines klar umrissenen Zwecks über die ganze Historie eines Datensatzes hinweg dürfte indessen für den Datenbearbeiter regelmässig sehr schwierig sein; die entsprechende Einwilligung ist aber erforderlich, ausser wenn – in Ausnahmefällen – die (persönlichkeitsverletzende) Datenbearbeitung auf anderen Rechtfertigungsgründen wie einer gesetzlichen Grundlage oder einem überwiegenden privaten oder öffentlichen Interesse beruht. Der Betreiber von Big Data Analysen wird also entweder umfassende Massnahmen zur Risikominimierung vorkehren oder das angepeilte Geschäftsmodell in Frage stellen müssen. Der Ansatz der Anonymisierung versagt, wenn das Geschäftsmodell nicht statistische Auswertungen von Daten, sondern das Profiling in den Mittelpunkt stellt. Es ist davon auszugehen, dass künftig das Profiling bei der wirtschaftlichen Nutzung von personennahen und personenbezogenen Daten weiter an Bedeutung gewinnen wird.

Weiter kann der Life Cycle von Daten im Kontext von Big Data zwischen Informationsanreicherung, Anonymisierung und Re-Identifizierung abwechselnd eine personenbezogene Qualität (sogar mit besonders schützenswertem Status) erreichen und auch verlieren, während die Daten die verschiedenen Bearbeitungsplattformen der verantwortlichen Datenbearbeiter durchlaufen. Auch in dieser Konstellation sind (ggf. aufwändige) technische Massnahmen zur Sicherstellung der Einhaltung der Datenschutzprinzipien unumgänglich.

Der Grundsatz der Datenminimierung kann ebenfalls in einem Spannungsverhältnis zu Big Data Praktiken, möglichst viele Daten zu sammeln und zu analysieren, stehen. Der präventive Charakter des aktuellen Datenschutzrechts impliziert, dass die Erhebung, das Sammeln und das Aufbewahren von personenbezogenen Daten ein Risiko darstellt und diese Tätigkeiten entsprechend einzuschränken sind. Der Grundsatz lautet: nur so viel wie nötig. Dieses Grundprinzip der Datenminimierung ist auch in die Revision des Datenschutzes („Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen („Privacy by Design" und „Privacy by Default") eingeflossen und somit Bestandteil des technischen Anforderungssets im Datenschutz.

Zwar kennt das Datenschutzrecht neben der Zweckbindung und der Einwilligung auch den Schutzgedanken des individuellen Nicht-Teilnehmens an einer Datensammlung (Opting-out). Wer auf diese Weise keine Daten herausgibt, wird aber ggf. mit anderweitigen negativen Folgen zu rechnen haben, z.B. bei der Bonitätsbeurteilung, beim Bewerbungsprozess oder der Prämienberechnung bei Krankenkassenzusatzleistungen: Wer keinen Tracker trägt, erhält gewisse Vergünstigungen von der Versicherung nicht; wer sich auf keinem beruflichen Netzwerk vorstellt, läuft Gefahr, als intransparenter und damit nicht valabler Kandidat eingestuft zu werden, oder wer bei Google Earth sein Haus verpixeln lässt, könnte Einbrecher dazu verleiten, dort vorbeizuschauen.

Die vorerwähnten Überlegungen und Beispiele zeigen: Neue Datenbearbeitungsverfahren, v.a. Big Data Analysen, schaffen das Potential von Spannungsfeldern mit den Datenschutzprinzipien. Indessen kann nur ein funktionierender Datenschutz das Vertrauen der Nutzer in die digitale Welt stärken und die Bereitschaft fördern, Daten zu teilen. Letztlich stellt sich somit die Frage, ob die moderne Ausgestaltung des Datenschutzes einen Kompromiss zwischen rechtskonformer Datenbearbeitung und günstigen Voraussetzungen für Big Data Analysen ermöglicht oder in ein Patt führt.

5.3.1.7 Mittel- und langfristige Entwicklung des Datenschutzes

Die technologische Revolution und Evolution, die Globalisierung der Datenbearbeitung und nicht zuletzt die schiere Menge und Vielfalt unstrukturierter Daten führen zur Frage nach der Zukunft des Schutzes der Privatsphäre und der informationellen Selbstbestimmung:

Zumindest kurz- bis mittelfristig dürften die aufgezeigten Instrumente des modernen Datenschutzes, wie sie in der Revision des DSG berücksichtigt sind, ihre Wirkung nicht verfehlen, sofern die Aufsichtsbehörde im Datenschutz (EDÖB) die dazu nötigen Mittel für Beratung, Kontrolle und Durchsetzung erhält. Vor diesem Hintergrund sind eine rasche Umsetzung der Datenschutzrevision ohne Verzögerungen und die vom Bundesrat in Aussicht gestellte Aufstockung der Ressourcen entscheidend.

Mittel- bis langfristig sind hingegen verschiedene Entwicklungen in Betracht zu ziehen, weshalb die Expertengruppe zwei Szenarien für die Zukunft des Datenschutzes erarbeitet hat.

Szenario I: Die heutigen Datenschutzprinzipien sind zukunftstauglich
Das erste Szenario geht davon aus, dass die technologieneutral formulierten Prinzipien des revidierten Datenschutzes sich auch in weiterer Zukunft als praktikabel erweisen und die Kernziele des Datenschutzes erreicht werden:

- Die materiellen Grundsätze des Datenschutzes werden von der Realität von Big Data und der KI nicht in Frage gestellt und erlauben eine zielführende und flexible Umsetzung im Alltag.
- Die Praxistauglichkeit und der Erfolg des Datenschutzes beruht auf dem bewährten Muster einer generell-abstrakten, hinreichend offenen Regulierung des Datenschutzrechts. Deren weiter Ermessensspielraum stärkt die Chancen und Möglichkeiten des Big Data, mit Blick auf das Sicherheits- und Vertrauensbedürfnis des Konsumenten und Nutzers, anstatt sie einzuschränken.
- Die schrittweise Lösungssuche und eine konstante Rechtsprechung lösen in den nächsten Jahren die aktuell noch zu konkretisierenden Umsetzungsfragen – etwa

bezüglich des „Privacy by Design“ Prinzips oder des „Rechts auf Vergessen“ – und sorgen für Rechtssicherheit.

Zusammengefasst erweist sich in diesem Szenario der Datenschutz mit dem Big Data-Ansatz als vereinbar. Der Datenschutz und die Rechtsprechung führen zu einem austarierten Verhältnis zwischen einem funktionierenden Schutz der Privatsphäre und der informationellen Selbstbestimmung sowie den Rahmenbedingungen für eine moderne Datenbearbeitung, die auch die Methoden von Big Data abdeckt.

Szenario II: Eingeschränkte Zukunftstauglichkeit der heutigen Datenschutzprinzipien

Vier Faktoren akzentuieren die Risiken mit Blick auf die Sicherstellung der Einhaltung der heutigen Datenschutzprinzipien:

- Die praktische Umsetzung der technologieneutral formulierten Grundprinzipien des Datenschutzes stösst bei den neuen Datenbearbeitungstechniken, insbesondere bei den Big Data Analysen, auf nicht zu unterschätzende Schwierigkeiten.
- Die Umsetzung der neuen Datenschutzprinzipien vermag aus heutiger Sicht die Unsicherheiten bei den Datenbearbeitern und den Betroffenen kaum zeitgerecht auszuräumen, wie die jüngsten Erfahrungen mit der Umsetzung der DSGVO gezeigt haben.
- Die Mehrheit der Nutzerinnen und Nutzer betont zwar die Wichtigkeit der Privatsphäre und der informationellen Selbstbestimmung, verzichtet aber im Alltag oft darauf, sich für die Wahrung dieser Rechte selbstverantwortlich zu engagieren.
- Im B2C-Bereich sind derzeit insbesondere Unternehmen marktbeherrschend, die ihre Geschäftsmodelle in einem Rechtssystem entwickeln, das dem Datenschutz nicht den gleichen Stellenwert wie Europa beimisst bzw. den Schutz des Individuums vor Datenmissbrauch anders sicherstellt.

Schlussfolgerungen aus den Szenarien I und II

Der nächste Schritt bei der Entwicklung des Datenschutzes ist entscheidend und muss mit der Revision schnellstmöglich abgeschlossen und konsequent umgesetzt werden; denn nur mit den vorgeschlagenen Anpassungen des Datenschutzes an die digitale Realität kann die Wirkung des traditionellen Datenschutzansatzes im Kontext moderner Datenbearbeitung überprüft werden. Auch wenn das Szenario I von einer günstigen Entwicklung ausgeht, sind die Herausforderungen nicht zu übersehen: Insbesondere die Regelung der neuen technischen Auflagen im Datenschutzgesetz wird bei den Verantwortlichen der Datenbearbeitung, aber auch bei den Nutzern zu Unsicherheiten führen.

Die jüngsten Zwischenfälle im Zusammenhang mit sozialen Netzwerken zeigen, dass die im Szenario II diskutierten Risiken durchaus real sind und in Zukunft noch weiter an Relevanz gewinnen dürften. Die datenschutztechnischen Herausforderungen im Spannungsdreieck zwischen den Kosten für eine rechtskonforme Umsetzung einer strengen Datenschutzumsetzung, den Chancen einer modernen Datenbearbeitung mittels Big Data und den negativen Folgen einer wenig strikten Umsetzung des Datenschutzes für den Schutz der Privatsphäre könnten in ein Dilemma münden. Zwischen dem Anspruch auf Privatsphäre auf der einen Seite und digitalem Komfort, Funktiona-

lität und sozialer Online-Teilhabe auf der anderen Seite werden sich die Nutzer entweder von der digitalen Welt zurückziehen oder Abstriche beim Schutz der Privatsphäre in Kauf nehmen müssen.

Vor diesem Hintergrund hat die Expertengruppe die Notwendigkeit gesehen, ergänzende Massnahmen zum Datenschutz und alternative Möglichkeiten zum Schutz der Privatsphäre und der informationellen Selbstbestimmung zu erörtern und zur Diskussion zu stellen.

5.3.1.8 Ergänzende Massnahmen zum Datenschutz und alternative Massnahmen im Datenschutz

Der erwähnte Angemessenheitsbeschluss der EU wirkt sich auch auf den Handlungsspielraum der Schweiz bei der Ausgestaltung des künftigen Datenschutzrechts aus. Dennoch seien folgende Überlegungen erlaubt: Lösungsansätze wie „Schweizweite Harmonisierung des Datenschutzes“, „Accountability-Prinzip“, „Smart Data-Ansatz“ „Sharing the Wealth-Prinzip“ und „Historisierung des Datenweges“ bewegen sich im Rahmen des traditionellen Datenschutzes; demgegenüber weisen alternative Ansätze wie die „Lockerung der Zweckbindung“ und dem Datenschutz nachgelagerte Rechtsmechanismen zwecks Schutz der betroffenen Person vor einem Datenmissbrauch über den traditionellen Datenschutz hinaus.

Ergänzende Massnahmen im Rahmen des traditionellen Datenschutzes:

a) Funktionsgrundrechte

Bereits heute zeichnet es sich ab, dass die Grundsätze der Privatsphäre in der Bundesverfassung (Art. 10 und 13 BV) nicht nur als Abwehrrecht gegenüber dem Staat, sondern als Funktionsgrundrechte zu verstehen sind. Das deutsche Bundesverfassungsgericht hat 2008 festgehalten, dass die Anbieter von Systemen und Infrastrukturen die Vertraulichkeit von Personendaten zu gewährleisten haben, was eine entsprechende technische Konkretisierung auch von Datenbearbeitungsgrundsätzen voraussetzt. Eine Änderung der Bundesverfassung drängt sich nicht auf. Die Expertengruppe würde es aber begrüssen, wenn die Rechtsprechung die informationelle Selbstbestimmung wie in Deutschland zu einem Funktionsgrundrecht weiterentwickeln würde.

b) Accountability-Prinzip

Das Accountability-Prinzip setzt beim Datenbearbeiter an und nimmt ihn verstärkt und verbindlich in die Pflicht, wobei viele Elemente des Prinzips bereits in den E-DSG eingeflossen sind. Ein Unternehmen kommt seiner Rechenschaftspflicht (accountability) nach, wenn es die Datenbearbeitung transparent gestaltet und einen Datenbearbeitungsstandard einhält. Neben der Transparenz wären das risikobasierte Vorgehen und Massnahmen der Informationssicherheit wichtige Elemente für den Standard. Schliesslich gehört es zur Accountability eines Unternehmens, den betroffenen Personen eine benutzerfreundliche Übersicht über sie betreffende Daten zu geben. Kontrollen - etwa durch einen mit angemessenen Mitteln ausgestatten EDÖB - würden wesentlich dazu beitragen, den Standard durchzusetzen. Weitere Massnahmen der guten Praxis wie etwa die Selbstverpflichtung zum Smart Data-Prinzip (s. weiter unten Smart Data-Ansatz) wären fortlaufend zu diskutieren. Der Accountability-Standard könnte die Grundlage für die im E-DSG vorgesehene Zertifizierung sein, was einem Qualitätssiegel für die Datenbearbeitung eines Unternehmens gleichkäme. Ebenso müsste die Möglichkeit zur Selbstzertifizierung gegeben werden, was bei den Unternehmen Selbstregulierung und Eigenverantwortung stärken könnte. In jedem Fall

müssten sich die Prinzipien einer erweiterten Accountability sowohl für die Regulierung als auch für das (Selbst)Zertifizierungssystem eignen.

c) Sandboxing (sichere Testumgebung)

Zu vertiefen ist die Frage, ob bei der Bearbeitung unstrukturierter Daten im Kontext neuer Geschäftsmodelle ein Sandboxing-Ansatz zielführend wäre. In diesen eng von den Aufsichtsbehörden begleiteten Testanordnungen mit Hilfe eines Testtools würde bei einer limitierten und inventarisierten Datenmenge (Volume) die Zweckbindung gelockert und eine Generaleinwilligung durch die betroffenen Personen ermöglicht. Die Komplexität von Big Data wäre deutlich reduziert. Die zugelassenen Formate der unstrukturierten Daten und deren Herkunft wären kontrolliert. Neben der Strukturierung des Datenpools müsste der Zugriff (link) des zu überprüfenden Programms auf diesen Datenpool gesteuert werden, ebenso welche Grössen (Parametrisierung) das Programm schliesslich ableitet und benutzt. Ebenfalls könnte man in dieser Testanordnung untersuchen, wie und wann sich anonymisierte Daten wieder reidentifizieren lassen.

Allerdings darf auch bei dieser reduzierten Anzahl von Daten mit einer kontrollierten Gruppe von Personen nicht ausgeschlossen werden, dass plötzlich Personen ausserhalb der Versuchsanordnung betroffen wären. So wäre vorstellbar, dass ein anonymisierter Datengeber eines Genoms im „Sandkasten“ reidentifiziert wird, dieses Genom auf eine Erbkrankheit hinweist und plötzlich auch seine erwachsenen Kinder ohne deren Einwilligung Teil der Versuchsanordnung werden.

Vor diesem Hintergrund hat die Testumgebung zwei übergeordnete Ziele: Sollen nur statistische Auswertungen im Vordergrund stehen, überprüft das Tool, ob aufgrund der erarbeiteten und allenfalls auch zu veröffentlichenden Statistiken personenbezogene Daten herausgelesen werden können („statistical Disclosure Control"). Im Kontext personenbezogener Daten wäre der Nutzen eine deutlich verbesserte Risikofolgenabschätzung, was dem Ansatz eines risikobasierten Datenschutzes zugutekäme.

Grundsätzlich wäre die Vereinbarkeit solcher Tools mit dem Datenschutz zu prüfen – insbesondere das Prinzip Zweckbindung könnte eine Herausforderung darstellen. Aufgrund der Sensitivität solcher Tools müsste ein detailliertes Rahmenwerk definiert werden. Hier böte sich an, dass u.a. die Aufsichtsbehörden im Datenschutz in Zusammenarbeit mit Forschung und Wirtschaft (Public-Private Partnership) solche Tools erarbeiten und anbieten würden.

d) Smart Data-Ansatz

Verschiedene datenschutzrechtliche Auflagen, insbesondere die Datenminimierung, stehen mit Big Data Analysen von grossen Volumina personenbezogener Daten in einem Spannungsverhältnis. Ein Ausweg ist der „Smart Data“- Ansatz, der versucht, mit möglichst wenig Daten auszukommen, die aber umso informativer sind. Allerdings widerspricht der Prozess der Korrelationssuche bei Big Data Analysen gerade der Idee, dass ein anfangs unbekannter Output der Analyse vorab über einen limitierten Input an Daten erreicht werden kann - ein Ansatz, der eher wieder zur Kausalitäts- und Thesenüberprüfung mit limitierten Datenvolumen und Stichproben führt.

e) Sharing the Wealth-Prinzip

Das „Sharing the Wealth“-Prinzip diskutiert die ökonomische Seite der Nutzung personenbezogener Daten. Es befriedigt das wirtschaftliche Partizipationsbedürfnis der Nutzer und ist deshalb als Massnahme zur Förderung der informationellen Selbstbestimmung anzusehen. Da hier der Aspekt der Datenportabilität wesentlich ist, wird der Ansatz „Sharing the Wealth“ in Ziff. 7.1.5.2 detaillierter ausgeführt.

f) Historisierbarkeit der Daten „Life Cycle“

Eine Schlüsselherausforderung des künftigen Datenschutzrechts ist die fehlende Rückverfolgbarkeit einer Information, die sich aus mindestens zwei Daten zusammensetzt (Data Life Cycle). Während Informationen und die dazugehörenden Daten früher in einem statischen Zustand verblieben, ermöglicht die heutige Bearbeitung eine dynamische Transformation der Daten. Sie können Sachdaten, personenbezogene Daten, anonymisierte Daten oder wieder reidentifizierte Daten sein. Je nach Zeitpunkt im Lebenszyklus von Daten ändert sich also deren rechtliche Kategorisierung.

Weiter wird die Datenbearbeitung zunehmend nicht mehr dort stattfinden, wo die Daten beschafft worden sind. Auf den ersten Blick scheint die Durchsetzbarkeit des Datenschutzes davon nicht betroffen zu sein. Rechtlich steht der Datenbearbeiter in der Verantwortung, der zu einem bestimmten Zeitpunkt personenbezogene Daten bearbeitet und gegen datenschutzrechtliche Prinzipien verstösst. Allerdings dürften komplexe Datenhistorien die Transparenz und Einwilligung erschweren und das Durchsetzungsniveau relativieren. Vor diesem Hintergrund wäre der technische Ansatz interessant, jeder festgehaltenen Information im Datensatz die Historie „mitzugeben“. Damit wäre eine Nachvollziehbarkeit gewährleistet. Bei einem Missbrauch von Daten, z.B. bei einer Reputationsschädigung, bestünde die Möglichkeit, den Ablauf zu rekonstruieren und die verantwortlichen Stellen zur Rechenschaft zu ziehen. In diesem Sinn ist die „Historisierung“ der Daten keine eigenständige Alternative, sondern ein weiteres Hilfsmittel, um dem Prinzip der Accountability Nachdruck zu verschaffen. Allerdings sind zurzeit entsprechende technische Konzepte theoretischer Art und noch weit entfernt von einer konkreten, geschweige denn alltagstauglichen Umsetzung. Ein technischer Ansatz wäre eine künftige Variante einer hocheffizienten Blockchain, die zurzeit aber nicht zur Verfügung steht.

g) Alternative Ansätze ausserhalb des Datenschutzgesetzes

Als Konsequenz aus den vorgenannten Überlegungen wäre ein über das klassische Verständnis des Datenschutzes - d.h. Schutz der Privatsphäre und Schutz vor Missbrauch persönlicher Daten - hinausgehendes Modell zu prüfen.

So wären ausserhalb des Datenschutzes nachgelagerte Rechtsmechanismen in Betracht zu ziehen, wo die digitale Datenbearbeitung und -nutzung zu Missbrauch und Diskriminierung führt. Dies kann bei der Bonität, im Versicherungswesen, bei der Personalbewirtschaftung, beim Bewerbungsprozess oder beim Ausschluss von Dienstleistungen und Informationen der Fall sein. Eine solche Benachteiligung wiegt besonders schwer, wenn durch die Machtstellung des Anbieters Ausweichmöglichkeiten fehlen, wenn Waren oder Dienstleistungen nicht allgemein und öffentlich angeboten werden, wenn die Dienstleistungen und Produkte zum Normalbedarf gehören oder wenn der Anbieter keine sachlich gerechtfertigten Gründe anführen kann. Diese neue Betrachtungsweise - weg von der Datenbeschaffung zur Datennutzung - böte auch dann Lösungspotenzial, wenn die Informationspflicht bei einer automatisierten Einzelentscheidung nicht greifen würde.

Im weitesten Sinn geht bereits die Regelung der Preisdifferenzierung im UWG und in der Preisbekanntgabeverordnung vom 11. Dezember 1978 (PBV) (s. Ziff. 5.3.2.5) in diese Richtung, indem sie die Preisdiskriminierung aufgreift. Schwieriger gestaltet sich das Problem, wenn die Daten zu einem „missbräuchlichen“ Ausschluss von Dienstleistungen und Informationen führten.

Dies wiegt besonders schwer, wenn die Dienstleistung wiederum Voraussetzung ist für gewisse Rechte, etwa den Abschluss einer Motorfahrzeug-Haftpflichtversicherung für die Inverkehrssetzung eines Autos. Die sogenannten Kontrahierungszwänge grei-

fen dieses Problem auf, sind aber besonders im privatrechtlichen Bereich nur mit grosser Zurückhaltung möglich. So darf der Nutzerin oder dem Nutzer keine andere zumutbare Ausweichmöglichkeit zur Verfügung stehen.

Es ist deshalb zu prüfen, ob solche oder andere Ansätze der Missbrauchsbeschränkung zielführend wären, in welchen Rechtsbereichen eine Anwendung Sinn machen würde und welche Anpassungen erfolgen müssten.

Empfehlung:

8. Der Bund setzt sich für eine Stärkung der informationellen Selbstbestimmung ein, fördert namentlich datenschutzfreundliche Technologien und prüft unter Berücksichtigung der internationalen Entwicklungen und des technischen Fortschritts ergänzende und alternative Ansätze inner- und ausserhalb des Datenschutzrechts.

5.3.1.9 Bedeutung von Scoring und Profiling bei Prozessen mit reduzierter Möglichkeit zur freiwilligen Einwilligung

Im arbeitsrechtlichen Bewerbungsverfahren ist der Arbeitgeber berechtigt, jene Informationen über den Bewerber zu bearbeiten, die er zur Klärung der Eignung für das Arbeitsverhältnis benötigt (Arbeitsplatzbezug). Alle weiteren Informationen, die der potenzielle neue Arbeitgeber nicht benötigt, darf er nicht bearbeiten (Verhältnismässigkeitsprinzip, Art. 328b OR). Wie auch das Einholen und Erteilen einer Referenz, haben Tracking, Profiling und Scoring im arbeitsrechtlichen Bewerbungsprozess rechtmässig sowie nach Treu und Glauben zu erfolgen. Weil dabei wesentliche Züge der Persönlichkeit des Bewerbers beurteilt werden (Profiling), ist für diese Art der Datenbearbeitung die vorgängige und ausdrückliche Einwilligung des Betroffenen erforderlich (Art. 4 Abs. 5 DSG). Diese ist jedoch im Arbeitsbereich generell mit einem grossen Vorbehalt versehen, fehlt es im Bewerbungsverfahren oder Arbeitsverhältnis doch regelmässig an der für die Gültigkeit der Einwilligung vorausgesetzten Freiwilligkeit.

Bei einem Bewerbungsverfahren für eine Aus- oder Weiterbildungsstelle kommen die arbeitsrechtlichen Bestimmungen nicht zur Anwendung, jedoch dürfte die Einwilligungsproblematik auch dort bestehen. Die datenschutzrechtlichen Anforderungen, insbesondere bezüglich Verhältnismässigkeit, Rechtmässigkeit sowie Treu und Glauben, müssen ebenfalls beachtet werden.

Sofern besonders schützenswerte Personendaten beschafft werden, ist zudem Art. 14 DSG zu beachten, wonach die betroffene Person zu informieren ist. Dies gilt auch dann, wenn die Daten bei Dritten beschafft werden. Denkbar ist dies zum Beispiel bei Personalvermittlungsdienstleistern oder grossen Personalabteilungen.

In diesen Bereichen wie auch im Gesundheitsbereich müssen die entsprechenden Spezialgesetze weiterentwickelt werden. Diese haben im Einklang mit dem Datenschutz zu stehen.

5.3.1.10 Strafrechtliche Herausforderungen

Die grösste Stärke der Applikationen droht gleichzeitig zu einem nicht kontrollierbaren Risiko zu werden, da Verschwiegenheit und Vertraulichkeit nicht mehr an eine Person im Sinne einer Mitarbeiterin oder eines Mitarbeiters in Vertrauensposition gebunden werden können. Wesentlich sind hier datenschutztechnische Fragen, nicht minder wichtig aber auch der Schutz von Geheimnissen. In dem Masse, wie die Aufgabenbreite und „Verantwortung“ dieser Applikationen steigt, stellt sich die Frage, ob die

rechtliche Regelung im Strafrecht (insbesondere Art. 162 und 321 StGB) die Verantwortung der Anbieter dieser Dienstleistungen adäquat abbildet und zuweist.

Empfehlung:

9. Der Bund prüft, ob die geltenden Strafnormen ausreichen, um bei der Verletzung von Geheimnissen durch digitale Systeme (z.B. durch personalisierte Applikationen) den Verursacher zur Verantwortung ziehen zu können.

5.3.1.11 Entwicklung des Datenschutzes und IKT-Sicherheit

Am 25. Mai 2018 lief die zweijährige Übergangsfrist für die DSGVO ab. Ab diesem Datum können einerseits die Einwohnerinnen und Einwohner der Schweiz gegenüber Bearbeitungsverantwortlichen in den EU-Staaten die verstärkten Schutzrechte der DSGVO geltend machen. Andererseits gilt die DSGVO für Schweizer Unternehmen, die Daten von Personen in der EU automatisiert und profilbildend bearbeiten. Diese haben die erforderlichen organisatorischen, technischen und rechtlichen Massnahmen im Hinblick auf die Konformität mit der DSGVO umzusetzen. Mit Blick auf den dem Datenschutz durch die Wirtschaft beigemessenen Stellenwert, der durch die Einführung der DSGVO und den darin vorgesehenen massiven Sanktionsmöglichkeiten sowie aufgrund der Revision des schweizerischen Datenschutzrechts allgemein gestiegen ist, ist der EDÖB als für die Privatwirtschaft allein zuständige Aufsichtsbehörde stark gefordert: Allein die Nachfrage von Beratungsleistungen und Begleitung von Projekten im Zusammenhang mit der digitalen Datenbearbeitung nimmt laufend zu. Eine Vielzahl von organisatorischen und technischen Massnahmen wie die Risikofolgenabschätzung, das Recht auf Löschung oder Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sind in die DSGVO eingeflossen. Als Bestandteil der formell-gesetzlichen Bestimmungen in der DSGVO haben diese Instrumente der IKT-Sicherheit zudem einen ungleich höheren Stellenwert erhalten. Sodann wurden die Pflichten im Hinblick auf die präventive Sicherstellung des Datenschutzes erheblich erweitert, wie z.B. betreffend Dokumentation der Datenverarbeitungstätigkeiten, Information der Betroffenen, Meldepflichten bei Datenschutz- und Sicherheitsvorfällen. Diese Instrumente sind aufgrund der Unterstellung von zahlreichen Schweizer Unternehmen unter die DSGVO bereits jetzt auch in der Schweiz Bestandteil der digitalen Gegenwart und werden mit der Revision des schweizerischen Datenschutzrechts mindestens zum Teil zusätzlich verankert und auch für rein auf den Schweizer Markt fokussierte Unternehmen verbindlich; entsprechend erweitert sich auch die Beratungs- und Aufsichtstätigkeit des EDÖB.

Gleichzeitig können die Möglichkeiten der modernen Datenverarbeitung durch Big Data Analysen, künstliche Intelligenz und Kryptografie ein durch die Technik verursachtes Risiko für den Datenschutz darstellen. Disziplinen wie IKT-Risikomanagement, Hardware basierte Sicherheit, Anonymisierung (insbesondere differential Privacy), Cloudlösungen und Kryptografie (zukünftig vor allem homomorphe Verschlüsselungen) werden noch wesentlich stärker interdisziplinär zusammengesetzte Datenschutzbehörden voraussetzen. Nur so werden sie den technischen und rechtlichen Herausforderungen der digitalen Grossbaustellen gleichermassen gewachsen sein.

Während der Bundesgesetzgeber mit der Ablösung des DSG aus dem Jahr 1993 noch am Anfang steht, sind die mit zusätzlichen Mitteln sowie Verfügungs- und Sanktionskompetenzen ausgestatteten Datenschutzbehörden der EU-Mitgliedstaaten daran, ihre Zusammenarbeit zu bündeln und gegebenenfalls auch gegenüber Unternehmen in Drittstaaten verstärkt zur Anwendung zu bringen. Das stellt die Datenschutzbehör-

den des Bundes und der Kantone vor die Herausforderung, in der schwierigen Übergangszeit bis zur Erneuerung des Schweizer Datenschutzrechts mit vergleichsweise bescheidenen Befugnissen und Ressourcen eine Aufsichtspräsenz zu entfalten, die im In- und Ausland als glaubwürdig und proaktiv wahrnehmbar ist. Die Mittel des EDÖB für den Datenschutz sind seit 2005 unverändert auf 24 Stellen beschränkt geblieben, und die Mittel in gewissen Kantonen fallen im Verhältnis sogar noch bescheidener aus.

Angesichts der Vielzahl von Datenverlust-Vorfällen, welche auch die digitale Realität in der Schweiz prägen, hat der Datenschutz demgegenüber in der öffentlichen Wahrnehmung stark an Bedeutung gewonnen.[9] Die Aufsichtsbehörden auf Bundes- und Kantonsebene sehen sich deshalb mit Erwartungen konfrontiert, die sich weder mit den gesetzlichen Grundlagen, noch mit den Ressourcen, die dem Stand des letzten Jahrhunderts entsprechen, glaubwürdig erfüllen lassen. Wirkungssteigerungen sind nicht nur durch zusätzliches Personal und Ausbildungsförderung, sondern auch durch Schaffung effizienter Kooperationsformen wie z.B. Kompetenzzentren herbeizuführen.

Empfehlungen:

10. Bund und Kantone passen die Ausstattung der Datenschutzbehörden mit Befugnissen und Mitteln so an, dass diese es ihnen ermöglichen, ihre gesetzlichen Aufgaben der Sensibilisierung, Beratung und Aufsicht umfassend und wirkungsvoll wahrnehmen zu können.
11. Der Bund schafft in Zusammenarbeit mit den Kantonen Kooperationsformen zwischen den Datenschutzaufsichtsbehörden (z.B. Kompetenzzentrum).

5.3.1.12 Standardisierung und Zertifizierung im Datenschutz

Cyber-physische Geräte beinhalten im Bereich des Datenschutzes ein hohes Risikopotenzial für die Persönlichkeit. Darunter fallen u.a. der Einsatz von Sensoren in der Medizininformatik (Apps auf dem Smartphone, aber auch industrielle Kontrollsysteme im medizintechnischen Bereich), Smartmeters, Baby Cams, Spielpuppen, die mit dem Internet verbunden sind – kurz alle Geräte, die Daten sammeln und verarbeiten, die sich auf Personen beziehen können. Im Unterschied zur Zertifizierung von Organisationen und Verfahren wurde der produktebezogene Ansatz im Rahmen des heute noch geltenden DSG nicht umgesetzt. Unter Berücksichtigung der technischen Ausgestaltung des neuen Datenschutzes muss ein solcher produkteorientierter Zertifizierungsansatz aufgenommen werden. Dieser muss insbesondere die datenschutzkonforme Gestaltung von Produkten („Privacy by Design“), datenschutzfreundliche Voreinstellungen („Privacy by Default“) und Sicherheitsauflagen („Security by Design“) berücksichtigen.

Mit Bezug auf den spezifischeren Datenschutz und mit Blick auf die DSGVO ist ein produkteorientierter Standardisierungs- und Zertifizierungsansatz zu prüfen. Dieser würde auf dem „Privacy by Design“ Prinzip beruhen und Elemente des „Security by Design“ aufnehmen. Für daran gekoppelte Marktzulassungsvoraussetzungen müssten entsprechende Rechtsgrundlagen erst noch geschaffen werden. Entsprechende Auflagen sind vor allem bei IoT-Geräten wichtig. Deren Vielfalt empfiehlt eine vertiefte Überprüfung, wo solche Zertifizierungen und Marktausschlüsse zielführend sind.

[9] S. u.a. Tätigkeitsbericht des EDÖB, 2017/2018. S. 6f.

Empfehlung:

12. Der Bund prüft mit Blick auf den Datenschutz und die Datensicherheit in Übereinstimmung mit den internationalen Entwicklungen und unter Berücksichtigung des Risikopotenzials und der Einsatzgebiete datenschutzkonforme Voreinstellungen.

5.3.2 Konsumentenschutz

5.3.2.1 Einführung

Das Akteurverhältnis B2C beleuchtet den Nutzer auch in seiner Rolle als Konsumenten in Bezug auf den Konsumentenschutz. B2C umfasst dabei privatwirtschaftliche Angebote wie auch Angebote staatsnaher Betriebe (SBB, Post, Swisscom). Mit Ausnahme einzelner gewerblicher Regulierungen sowie Konzessionierungsauflagen auf kantonaler Ebene gibt es bezüglich des Konsumentenschutzes keine Qualitätsauflagen. Ein entsprechender Qualitätslevel soll durch den Wettbewerb sichergestellt werden. Wesentliche Bestandteile des schweizerischen Konsumentenschutzes sind die Preistransparenz und der Schutz vor Betrug und Täuschung. Die Expertengruppe sieht zurzeit keine Notwendigkeit für einen allgemeinen Paradigmenwechsel. Auch in der digitalen Transformation scheint dieser Lösungsansatz des Konsumentenschutzes nach wie vor zu greifen. Anpassungen und eine Verbesserung der Durchsetzung des aktuellen Rechts drängen sich hingegen bei den Allgemeinen Geschäftsbedingungen (Ziff. 5.3.2.2), beim Widerrufsrecht (Ziff. 5.3.2.2), beim Digitalen Vertragsrecht (Ziff. 5.3.2.3), bei der Preisdifferenzierung (Ziff. 5.3.2.5) und bei der Online-Streiterledigung (Ziff. 5.3.2.6) auf.

Wichtig für die Konsumentinnen und Konsumenten in Bezug auf die Rechtsdurchsetzung in einem globalen Anbietermarkt sind die Frage des Gerichtsstandes und die Einführung eines „Marktortprinzips“ bei Anbietern ohne Domizil in der Schweiz. Die Durchsetzung eines Zustellungsdomizils, wie es jetzt im Parlament mehrfach verlangt wurde, muss geprüft werden, obwohl auf den ersten Blick die Erzwingbarkeit gegenüber den entsprechenden Internetfirmen im Ausland schwierig erscheint: Sanktionen in Form eines Marktausschlusses marktbeherrschender sozialer Netzwerke dürften vor allem auf breite Ablehnung der betroffenen Nutzer führen und gesellschaftspolitisch zu mehr Schaden führen als Wirkung erzielen. Bei aller Kritik zeigen erste Erfahrungen mit dem Gesetz vom 30. Juni 2017 zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz) in Deutschland aber, dass nur schon der Aufbau einer reputationsschädlichen Drohkulisse Wirkung zeigt. Die gesetzliche Verpflichtung der sozialen Netzwerke, im In- und Ausland einen verantwortlichen Ansprechpartner zu ernennen, gibt dem Geschädigten die Möglichkeit, gegen eine konkrete und adressierbare Entität gerichtlich vorzugehen.

5.3.2.2 Online-Geschäftsbedingungen

Online-Geschäftsbedingungen sind Allgemeine Geschäftsbedingungen (AGB), die nur Vertragsbestandteil werden können, wenn beide Vertragsseiten (insbesondere also auch der Abnehmer) ihnen zustimmen. In den digitalen Geschäftsmodellen gewinnen die Allgemeinen Geschäftsbedingungen (AGB) an Bedeutung; einseitig zugunsten des Anbieters formulierte AGB erweisen sich dabei als Problem.

Die Schweiz hat die Richtlinie 93/13/EWG über missbräuchliche Klauseln in Verbraucherverträgen nicht übernommen; angesichts des Widerstands in der Wirtschaft ist es

nur zur relativ schwachen Kontrollvorschrift in Art. 8 UWG gekommen. Vertragliche Sonderregeln für Online-AGB fehlen überhaupt. Das Schrifttum hat aber gewisse Kriterien entwickelt, die einzuhalten sind, damit Online-AGB zum Vertragsinhalt werden, etwa die gute Lesbarkeit, die Übersichtlichkeit, die sichtbare Darstellung und der vertretbare Umfang. Rechtsprechung zu diesen Kriterien gibt es aber kaum, und in der Realität erfolgt deren Beachtung nur beschränkt.

Im Datenschutzrecht spielt die benutzerfreundliche Ausgestaltung von Online-AGB inklusive Datenschutzbestimmungen indessen eine besondere Rolle; unter Berufung auf den Transparenzgrundsatz fordert die Datenschutzaufsicht die Erfüllung dieses Anliegens. Die Problematik liegt dabei weniger im Vorhandensein von Rechtsregeln als in deren Durchsetzung, weil es oft an den Mitteln für angemessene Beratungsdienste und Kontrollaufgaben fehlt. Mit der neuen DSGVO und künftig voraussichtlich auch mit dem neuen DSG steigen aber die Anforderungen, welche an die Übernahme von Online-AGB gestellt werden.

Empfehlung:

13. Der Bund setzt sich in Zusammenarbeit mit der Wirtschaft für die Einführung von Instrumenten ein, die zum Ziel haben, im Zusammenhang mit Online-AGB einen angemessenen Konsumentenschutz zu gewährleisten.

5.3.2.3 Online-Widerrufsrecht

Die Schweiz kennt Sonderregeln zum konsumentenrelevanten Widerrufsrecht bei sog. Haustürgeschäften (Art. 40a-40f OR). Diese Bestimmungen sind jedoch nach allgemeiner Auffassung auf Internetangebote und elektronische Vertragsabschlüsse aufgrund der engen Umschreibung der Voraussetzungen, insbesondere wegen der fehlenden physischen Präsenz der Vertragsparteien, nicht anwendbar.

Die EU hat bereits 2002 mit der Fernabsatz-Richtlinie 2002/65/EG ein Widerrufsrecht für Verbraucherverträge eingeführt, mit Ausnahme solcher Geschäfte, die ihrer Natur nach nicht widerrufsfähig sind. Mit einem neuen Richtlinien-Entwurf vom Dezember 2005 („Directive related to Online and Other Distance Sales of Goods“) will die EU die Rahmenbedingungen für Online-Verbraucherverträge einschliesslich des Widerrufsrechts konkretisieren und teilweise ausbauen; mit der Verabschiedung dieser Richtlinie ist im 2. Halbjahr 2018 zu rechnen, weil es keinen grundsätzlichen Widerstand gegen die neuen Vorschläge gibt.

Eine Gesetzesänderung, die für die Schweiz die Einführung eines Widerrufsrechts für Online-Geschäfte vorgesehen hätte, ist kürzlich erneut gescheitert. Eine Regelung zu den digitalen Inhalten im Vertragsrecht drängt sich aber auch für die Schweiz auf.

Empfehlung:

14. Der Bund prüft die Frage, ob ein angemessenes Widerrufsrecht bei Online-Geschäften einzuführen ist.

5.3.2.4 Digitales Vertragsrecht

Die neu entwickelten Geschäftsmodelle betreffen das Vertragsrecht in verschiedenster Weise.

a) Elektronischer Vertragsabschluss

Die durch das Internet schon vor über 20 Jahren eröffnete Möglichkeit, Verträge elektronisch abzuschliessen, hat den Gesetzgeber vor die Frage gestellt, ob es zusätzlicher Regeln zum Vertragsabschluss bedarf. Auf internationaler Ebene ist nach einem UN-CITRAL-Modellgesetz zum elektronischen Geschäftsverkehr das UN-Übereinkommen zu den elektronischen Kommunikationen (2005) entstanden, das die Schweiz aber bisher nicht ratifiziert hat. Die EU ist mit dem Erlass der E-Commerce-Richtlinie 2000/31/EG, welche die wichtigsten Aspekte mit Bezug auf elektronische Verträge regelt, aktiv geworden. Vorgesehen sind insbesondere die Gleichstellung der elektronischen mit den konventionellen Verträgen sowie spezifische Schutzvorschriften zum Vertragsabschluss. Das EJPD hat im Anschluss an den Erlass der E-Commerce-Richtlinie ein Vorprojekt für ein Bundesgesetz über den elektronischen Geschäftsverkehr mit ähnlichen Bestimmungen in die Vernehmlassung gegeben (2001); angesichts vieler negativer Reaktionen seitens der betroffenen Kreise ist es aber 2005 zum definitiven Abbruch der Bemühungen gekommen.

Die vergangenen 20 Jahre haben gezeigt, dass ungeachtet gewisser Besonderheiten des elektronischen Vertragsabschlusses die herkömmlichen Regeln des OR ausreichen, um sachgerechte Lösungen zu verwirklichen. Fragen des Zugangs einer Willenserklärung im Netz (Anwesenheit oder Abwesenheit, Dauer der Verbindlichkeit eines Angebots, Zeitpunkt des Vertragsabschlusses) sowie der Anfechtung mangelhafter Willenserklärungen lassen sich gestützt auf die bisherigen OR-Regeln beurteilen.

Einzig die Erfüllung des Schriftformerfordernisses, soweit es gesetzlich vorgeschrieben ist (z.B. einzelne Konsumentenverträge, Abtretung), hat einen Handlungsbedarf nach sich gezogen. Im Nachgang zur EU-Richtlinie über die elektronische Signatur (1999/93/EG) hat der Bundesrat die Zertifizierungsdienste-Verordnung erlassen, welche später durch das ZertES abgelöst wurde. Hingegen ist ein autonomer Nachvollzug der neueren EU-Verordnung über elektronische Identifizierung und Vertrauensdienste (EU) Nr.910/2014 (in Kraft seit 1. Juli 2016) bisher nicht erfolgt. Im Zusammenhang mit der Schaffung der E-Identität (E-ID) wäre aber die Einführung einzelner Bestimmungen durchaus denkbar.

b) Digitale Verträge und digitale Inhalte

In den letzten Jahren hat die Bedeutung der Digitalisierung im Kontext der Verträge zugenommen; abgesehen vom Einsatz neuer Technologien wie „distributed Ledger Technology“ (Blockchain) stehen die Daten bzw. Informationen, die Vertragsgegenstand sind und einen gewissen Wert repräsentieren, im Vordergrund.

c) Smart Contracts

Die Blockchain-Technologie ermöglicht eine vernetzte und selbstausführende algorithmische Begründung von Vertragsbeziehungen; anstelle der Aushandlung des Vertragstextes wird auf bereits getroffene Vereinbarungen in einem „Source Code “ Bezug genommen. Oft findet dabei der Begriff des sogenannten „Smart Contract“ Verwendung.

„Smarts Contracts“ verursachen einzelne Rechtsprobleme, die sich nicht ohne weiteres mit dem traditionellen Vertragsrecht bewältigen lassen. Dazu gehört etwa die Tatsache, dass die Durchsetzbarkeit nur innerhalb der Blockchain möglich ist und ein dezentrales länderübergreifendes System Fragen der Rechtszuständigkeit aufwirft. Ein gewisser regulatorischer Handlungsbedarf ist deshalb gegeben. (s. Ziff. 9.3.5).

d) Daten als Vertragsgegenstand: Digitale Inhalte

Schon traditionell haben Daten als Gegenstand von Verträgen fungiert, etwa im Falle des Kaufs bestimmter Informationen. Mit der Digitalisierung haben sich deshalb nicht

das Prinzip, sondern die Qualität und die Quantität des Auftretens solcher Vertragsinhalte geändert. Sonderfragen stellen sich auch mit Bezug auf die technische Übermittlung des Vertragsgegenstandes (Format, Standardisierung). Wenn aber Daten immer häufiger als Vertragsgegenstand auftreten, steigt auch das Risiko, dass Datenlieferungen die vertraglichen Qualitätskriterien nicht einhalten und Rechtsbehelfe wegen „Schlechtlieferung“ vorhanden sein müssen. Das heutige Recht ist auf diese Anforderungen schlecht vorbereitet.

Im Dezember 2015 hat die EU einen Vorschlag für eine neue Richtlinie zu digitalen Vertragsinhalten präsentiert („Directive concerning Contracts for the Supply of Digital Content“, COM(2015 634 fnal). Der Entwurf enthält eine Umschreibung des Begriffs „digitaler Inhalt“: Erfasst sind alle Güter in digitaler Form, z.B. Video, Audio, Apps, digitale Spiele oder andere Software sowie alle damit zusammenhängenden Dienstleistungen. Transaktionen über soziale Netzwerke und digitale Handelsplattformen fallen somit in den Anwendungsbereich der künftigen Richtlinie. Gewisse Ausnahmen sind ausdrücklich aufgelistet, ändern aber an der breiten Umschreibung der digitalen Inhalte wenig.

e) Konformitätsbeurteilung bei digitalen Vertragsinhalten

Die traditionellen OR-Regelungen zu den Rechtsbehelfen bei nichtkonformer Vertragserfüllung sind nicht auf digitale Vertragsinhalte zugeschnitten. Insbesondere der Begriff der Schlechterfüllung passt lediglich für Sachlieferungen und ggf. Dienstleistungen. Der Richtlinienentwurf der EU zu den digitalen Vertragsinhalten sieht deshalb neue Regelungen zur Vertragskonformität vor.

In der Praxis von Bedeutung ist dabei insbesondere die genaue vertragliche Umschreibung des Vertragsinhalts bzw. des Zwecks, den der Kunde mit dem Erwerb des digitalen Inhalts (Daten, Informationen) anstrebt, weil der beabsichtigte Verwendungszweck der Ausgangspunkt der Konformitätsbeurteilung ist. Nur im Falle der ausreichenden Konkretisierung des Vertragsgegenstands lässt sich hernach beurteilen, ob der digitale Vertragsinhalt die Erwartungen des Abnehmers erfüllt.

Weitere Fragen stellen sich mit Bezug auf die Intensität des „Gebrauchs“ digitaler Vertragsinhalte, weil der „Gebrauch“ die digitalen Güter (im Gegensatz zum „Gebrauch“ von Sachgütern) qualitativ und quantitativ nicht beeinträchtigt, sowie mit Bezug auf das Recht des Kunden, digitale Vertragsinhalte an Drittpersonen weiterzugeben. Schwierig sein kann in diesem Zusammenhang insbesondere die Abgrenzung zu vorhandenen Urheberrechten. Wenn die Informationen auch Personendaten von Dritten umfassen, vermag zusätzlich das Datenschutzrecht eine Rolle zu spielen.

Zudem erweisen sich spezifische Regelungen zu den Rechtsbehelfen als notwendig. Ist der digitale Vertragsinhalt unbrauchbar und kommt es zu einer Vertragsaufhebung, ist eine Rückerstattung der Daten in einem standardisierten Format vorzunehmen. Im Falle einer nicht so weitreichenden Abweichung von der vertraglich in Aussicht gestellten Qualität kommt eine Kaufpreisminderung in Frage; die quantitative Berechnung des Minderwerts des digitalen Vertragsinhalts verursacht aber regelmässig Schwierigkeiten.

In den letzten Monaten sind die Vorschläge der EU nicht nur von den interessierten Kreisen, sondern auch von den Mitgliedstaaten intensiv diskutiert worden. Die Regulierungsvorschläge zur Vertragskonformität und zu den Rechtsbehelfen greifen in die grundsätzlich den Mitgliedstaaten zustehende Gesetzgebungskompetenz im Vertragsrecht ein, was teilweise kritisch beurteilt wird. Welche konkreten Vorschläge der EU-Kommission deshalb einen Niederschlag in der im 2. Halbjahr 2018 zu verabschiedenden Richtlinie finden werden, lässt sich derzeit kaum abschätzen.

Die Schweiz kennt, wie erwähnt, überhaupt keine Bestimmungen zur Konformität von digitalen Vertragsinhalten sowie zu den möglichen Rechtsbehelfen. Je nach Ausgang der Diskussionen zur EU-Richtlinie wäre aber auch in der Schweiz zu erwägen, das OR durch zusätzliche Bestimmungen zu ergänzen.

Empfehlung:

15. Der Bund prüft für digitale Verträge und Inhalte unter Berücksichtigung der internationalen Entwicklungen, ob Anpassungen im Vertragsrecht nötig sind.

5.3.2.5 Irreführende und herabsetzende Handlungsweisen: Anpassungsbedarf im UWG

Das heutige Recht kennt eine lange Liste von irreführenden und herabsetzenden Handlungsweisen in Art. 3 UWG. Die neuen Geschäftsmodelle dürften durch diese detaillierten Normen weitgehend sinnvoll abgedeckt werden können (zur Übernahme marktreifer Ergebnisse s. auch Ziff. 6.3.3).

5.3.2.6 Preisdifferenzierung: Anpassungsbedarf im Wettbewerbsrecht und in der Preisbekanntgabeverordnung

Genauer zu prüfen ist die Frage der Preisdifferenzierung aufgrund von Datenanalysen mit einer allfälligen entsprechenden Anpassung der Preisbekanntgabeverordnung (PBV), insbesondere mit Blick auf die Transparenz und die Offenlegung der Mechanismen. Bei personalisierter Preisdifferenzierung stellt sich das Problem der Diskriminierung (beispielsweise dürften Rassenkriterien nach Art. 261bis StGB problematisch sein); zudem sind die Grundprinzipien des Datenschutzrechts zu beachten (Einschränkungen des Profiling, Einschränkungen bei „automatisierten Entscheiden“ gemäss DSGVO). Nach den Art. 16 ff. UWG und der darauf beruhenden PBV müssen die tatsächlich zu bezahlenden Preise gegenüber den Konsumenten bekanntgegeben werden. Damit soll einerseits klar sein, was das Angebot effektiv kostet (inklusive Zuschläge, Abgaben und Gebühren), und andererseits soll auch ein Preisvergleich möglich sein. Ersteres ist für das korrekte Zustandekommen des Vertrags notwendig (übereinstimmender Wille über Kernelemente), letzteres für einen funktionierenden Wettbewerb.

Implizit geht die PBV von konstanten und für alle Kunden gleichen Preisen aus, was zunehmend weniger der Fall ist. Zwar sind dynamische wie personalisierte Preise nicht neu (z.B. Saisonpreise, tiefere Preise vor Geschäftsschluss, AHV- oder Studentenrabatte, Stammkundenrabatte) und entsprechen einem wettbewerblichen Verhalten der Preisdifferenzierung nach Zahlungsbereitschaft. Sofern sie nicht auf einer monopolistischen Situation beruhen, sind sie in der Regel ökonomisch wohlfahrtsmehrend. Mit der Erfassung von immer mehr Daten, welche sich auf immer differenziertere Merkmale beziehen, werden dynamische wie personalisierte Preise aber in grösserem Umfang und bei immer mehr Angeboten möglich, sowohl online wie im Laden. Damit wird die wettbewerbliche Funktion der PBV allenfalls unterlaufen. Immerhin erlauben heute mögliche Datenanalysen auch verbesserte und raffiniertere Preisvergleiche. Die Problematik soll daher eher mit spezifischen Regeln angegangen und auf Sektoren mit besonderem Schutzinteresse wie etwa Grundversorgung oder Sozialschutz beschränkt (z.B. welche Faktoren für die Berechnung von Krankenkassenprämien berücksichtigt werden dürfen) und nicht flächendeckend etwa im Vertragsrecht oder im UWG angegangen werden. Bei der konkreten Analyse von dynamischen Preisen stellen sich zudem vertragsrechtliche Fragen und datenschutzrechtliche Herausforderungen (s. Ziff. 5.3.1.7).

Empfehlung:

16. Der Bund prüft, ob mittelfristig sektorspezifische Regulierungen, z.B. im Wettbewerbsrecht (UWG), in der Preisbekanntgabeverordnung oder im Versicherungsrecht nötig sind.

5.3.2.7 Online-Streiterledigung

Seit Beginn des Jahres 2017 kennt die EU eine funktionierende, wenn zwar bisher nur beschränkte Wirkung entfaltende „Online Dispute Resolution“ (für Konsumenten). Die Übernahme ähnlicher Regeln wäre wohl auch für die Schweiz empfehlenswert; das Thema ist zumindest zu vertiefen.

Die Online-Streiterledigung ist an sich nicht auf ein bestimmtes Rechtsgebiet beschränkt, aber sie hat im Kontext des (digitalen) Vertragsrechts die grösste praktische Bedeutung. Die EU befasst sich seit über 20 Jahren mit dem Thema der alternativen Streiterledigung („alternative Dispute Resolution“). Neue Formen der Streiterledigung erweisen sich insbesondere dann als sinnvoll, wenn die ordentliche staatliche Gerichtsbarkeit zu langsam und/oder zu teuer ist, was mit Blick auf digitale Transaktionen mit beschränktem Wert durchaus zutreffen kann. Abgesehen von der „physischen“ alternativen Streiterledigung hat das Anliegen, auch über Online-Formen zu verfügen, grössere Bedeutung erlangt.

Mit der in den EU-Mitgliedstaaten direkt anwendbaren Verordnung (EU) Nr. 524/2013 zur Online-Streiterledigung in Konsumentenangelegenheiten („Regulation on Dispute Resolution for Consumer Disputes“) hat die EU die Rahmenbedingungen für solche Verfahren festgelegt. Eine Ergänzung der Vorschriften ist durch die Implementierungs-Verordnung 2015/1051 erfolgt, welche die Modalitäten für die Ausübung von Funktionen im Rahmen der Online-Streiterledigungs-Plattform, für die Einreichung elektronischer Beschwerdeformulare und die Zusammenarbeit zwischen einzelnen Plattformen festlegt. Die Europäische Kommission hat zwischenzeitlich diese „Online Dispute Resolution (ODR)“ Plattform geschaffen und im Februar 2016 in Betrieb genommen.

Die ODR-Plattform unterscheidet vier Verfahrensschritte, nämlich die Einreichung einer Beschwerde („Klage“), die Übereinkunft der Parteien bezüglich der Streiterledigungsstelle, die Verfahrensführung durch die Streiterledigungsstelle sowie den Entscheid und den Verfahrensabschluss. Die EU-Mitgliedstaaten sind verpflichtet, nationale „Kontaktpunkte“ zu schaffen, welche die Konsumenten bei der Benutzung der ODR Plattform unterstützen. Die Erfahrungen mit der neuen ODR-Plattform sind zeitbedingt noch beschränkt. Für die Schweiz stellt sich aber die Frage, ob es nicht sinnvoll wäre, eine ähnliche „Institution“ einzurichten.

Empfehlung:

17. Der Bund fördert Online-Beschwerde- und -Streitschlichtungsmechanismen (Online Dispute Resolution, ODR), unter Einbezug privater Angebote.

5.3.2.8 Geoblocking

Mit „Geoblocking“ schliessen Anbieter Nachfrager ausserhalb eines definierten Raumes von der Nutzung von Angeboten im Internet aus. Beispielsweise werden Schweizer Konsumenten in einem deutschen Webshop nicht bedient oder auf eine andere (Schweizer) Webseite verwiesen. Gründe für ein „Geoblocking“ liegen etwa in der Durchsetzung einer Preisdifferenzierung (geografische Preisdiskriminierung), in der Vermeidung administrativer Abwicklung (z.B. Verzollung), in Zulassungsbedingungen,

in der Beachtung von Immaterialgüterrechten oder Lizenzbestimmungen (z.B. werden Urheberrechtslizenzen etwa für Filme oft territorial eingeschränkt) oder auch in weiteren gesetzlichen Rahmenbedingungen (weitergehende Konsumentenrechte wie Garantiebestimmungen oder Restriktionen für den Vertrieb von bestimmten Finanzprodukten).

Innerhalb der EU soll das „Geoblocking“ mit einer Verordnung im Sinne der Durchsetzung eines einheitlichen Binnenmarktes grundsätzlich untersagt werden. Wer in einem Mitgliedstaat Produkte oder Dienstleistungen im Internet anbietet, muss diese im Grundsatz auch Nachfragenden aus anderen Mitgliedstaaten im Internet anbieten. Die Verordnung sieht allerdings nach heutigem Stand verschiedene Ausnahmen vor, etwa zur Respektierung territorialer Urheberrechte, zur Anwendung der Konsumentenbestimmungen im Ursprungs- statt im Bestimmungsland oder zur Lieferpflicht ins Ausland.

In der Schweiz kann „Geoblocking“ unter Umständen kartellrechtlich erfasst sein, z.B, wenn Marktmacht vorliegt (nach Art. 7 KG) oder bei einem vertikalen Vertriebssystem (nach Art. 5 Abs. 4 KG), wobei keine rechtskräftigen Entscheide vorliegen. Die Volksinitiative „Für Faire Preise“ verlangt zusätzlich eine Regelung im UWG, ohne diesen Anspruch aber zu konkretisieren.

5.3.2.9 Netzsperren

Grundsätzlich ist das Internet offen ausgerichtet und mit seinem Netzcharakter wenig abgeschottet. Daten und Informationen werden in Paketen über verschiedene Knoten (Server) vom Anbieter zum Empfänger geleitet. Mit Netzsperren sollen unerwünschte Angebote staatlich dennoch verhindert werden, indem der Zugang auf die entsprechenden Adresselemente technisch blockiert wird. In der Regel funktionieren sie so, dass staatliche Behörden Internetdienstleister anweisen, die Verbindung zu bestimmten Servern zu blockieren (gleichsam wie eine Strassensperre). Solche Blockaden können allerdings mit einfachen technischen Mitteln umgangen werden (z.B. Anonymisierung von Servern oder virtuelle private Netzwerke VPN), welche frei zugänglich sind. Netzsperren werden von verschiedenen Ländern eingesetzt, um etwa (private) Immaterialgüterrechte (meist Urheberrechte) durchzusetzen, im betreffenden Land unzulässige Angebote zu blockieren (z.B. Geldspiele), gegen Kinderpornografie vorzugehen oder staatsgefährdende Aktivitäten (Terrorismus, teils aber auch „staatsfeindliche“ Information) zu unterbinden. In der Schweiz werden Netzsperren gegen Kinderpornografie aufgrund einer freiwilligen Befolgung einer staatlichen Sperrliste eingesetzt. Das neue Geldspielgesetz vom 29. September 2017 (BGS) schafft die Möglichkeit, den Zugang zu in der Schweiz nicht bewilligten ausländischen Online-Spielangeboten zu sperren. In die Revision des Urheberrechts wurde der Vorschlag von Netzsperren nicht aufgenommen.

Diskutiert wurde die verfassungsrechtliche Zulässigkeit von Zugangssperren im Bereich der Geldspiele. Das Bundesamt für Justiz geht in einem Gutachten davon aus, dass Zugangssperren jedenfalls in diesem Bereich zulässig sind.[10] Anderer Meinung ist ein Gutachten aus der Lehre[11]. Die Bundesversammlung ist in der Folge dem Bundesrat gefolgt und hat beschlossen, im Bereich der Geldspiele Zugangssperren zu

[10] Vgl. dazu den Bericht des Bundesamtes für Justiz vom 4. Juli 2017, "Internetsperre" und ihre Alternativen, mit zahlreichen Hinweisen (https://www.bj.admin.ch/dam/data/bj/wirtschaft/gesetzgebung/geldspielgesetz/notiz-internetsperre-d.pdf). Von der Verfassungsmässigkeit aus geht nun auch Giovanni Biaggini, BV Kommentar, 2. Auflage Zürich 2017, Rz. 6 zu Artikel 106.

[11] Vgl. Gutachten Florent Thouvenin/Burkhard Stiller vom 16. Sept. 2016, publiziert in sic! 2017 S. 701 ff.

verankern.

Kritisiert wird im politischen Diskurs und in der Fachliteratur, dass Zugangssperren leicht umgangen werden können. In der Praxis können sie zudem auch überschiessende Wirkung entfalten, indem mit der Blockade von Adresselementen von Servern auch legitime Angebote ausgeschlossen werden. Aufgrund der dynamischen Ausgestaltung des Internets werden Netzsperren zudem meist von Verwaltungsbehörden und ohne Rechtsmittel verfügt, was wegen einer zeitgerechten Wirkung plausibel erscheint, rechtsstaatlich aber problematisch ist. Netzsperren sollen daher nur in absoluten Ausnahmefällen über die Bereiche der Kinderpornografie oder der Geldspiele hinaus erwogen werden und bedürfen einer sehr strikten kritischen Überprüfung sowie eines gerichtlichen Verfahrens.

6 Analysefeld Business to Business (B2B)

6.1 Ist-Zustand und weitere Entwicklung

Die digitale Transformation führt volkswirtschaftlich betrachtet zu einem Wirtschaftswachstum, verursacht aber auch einen Strukturwandel. Faktoren sind dabei die Erhöhung des Sachkapitals und der Produktivitätsanstieg (Bericht des Bundesrats vom 11. November 2017, S. 18 ff). Die Digitalisierung führt zu tieferen Transaktionskosten, zur leichteren Nutzung von Skalenerträgen und zu einer grösseren Anzahl potentieller Marktteilnehmer. Das Stichwort lautet „Disintermediation", verbunden mit einer steigenden Bedeutung von Netzwerkeffekten. Dieser rasche Wandel hat die Entwicklung neuer Geschäftsmodelle und neuer Angebote ermöglicht.

Daten sind heute nicht mehr und künftig immer weniger nur Informationsträger, sondern ebenso sehr ein Wert-Gut. Damit erhalten die Daten eine gesteigerte wirtschaftliche Bedeutung; in der Folge lassen sich Daten im Austausch als „Zahlungsmittel" einsetzen. Zu prüfen ist deshalb, ob und in welcher Form diese neue Realität in der Ausgestaltung der rechtlichen Rahmenbedingungen ihren Niederschlag finden sollte. Die Grundprinzipien einer sozialen Marktwirtschaftsordnung, wie sie die Schweiz kennt und wie sie in der Bundesverfassung verankert sind (Art. 94 BV), beruhen auf der Privatinitiative bzw. den unternehmerischen Anreizen und subsidiären staatlichen Eingriffen, falls ein Korrekturbedarf besteht. Wertschöpfung und Arbeitsplätze erreichen dabei das erhoffte Steigerungspotential in der Wohlstandsförderung, wenn die künftigen Technologieentwicklungen und die Innovationen nicht durch Regulierungen übermässig eingeschränkt oder fehlgeleitet werden. Eine offene und liberale Regulierung kann sich ändernden Verhältnissen besser anpassen als strikte Staatsinterventionen.

Der B2B-Bereich zeichnet sich, gerade angesichts der digitalen Transformation, durch eine besonders starke internationale Vernetzung aus. Digitale Infrastrukturen sind heute global, Daten lassen sich an beliebig vielen Orten herunterladen. Überdies sind Informationen unbeschränkt reproduzierbar, werden also – im Gegensatz zu den Gütern – nicht durch den einmaligen Gebrauch „konsumiert", wenn nicht spezifische Schutzmassnahmen (z.B. Urheberrecht) zur Anwendung gelangen.

Die Tatsache der Internationalität des Datenflusses schränkt die Handlungsoptionen des Schweizer Gesetzgebers erheblich ein; künftig werden „Insellösungen" für die Schweiz im digitalen B2B-Bereich, ohne gleichzeitig massive Kollateralschäden zu verursachen (Netzsperren), immer weniger möglich sein.

Der Arbeitsmarkt wird durch die digitale Transformation stark beeinflusst und zwar in unterschiedlichen Richtungen. Namhafte Verschiebungen zwischen Berufsgruppen, den Sektoren und Branchen sowie in der Art der Beschäftigung (Selbstständige / Arbeitnehmer) sind zu erwarten. Neue Formen der Zusammenarbeit (Kollaboration) erbringen Mehrwert und Chancen, stellen aber auch neue Herausforderungen an Arbeitnehmer und Arbeitgeber. All dies hat zur Folge, dass Qualifikationsanforderungen (berufliche Ausbildung und Beschäftigungsprofile) erheblichen Veränderungen ausgesetzt sein dürften. Bestehende Schutznormen müssen in einem neuen Zusammenhang beurteilt werden. Abgesehen von strukturellen und inhaltlichen Veränderungen bringt die digitale Transformation auch neue Möglichkeiten zur vermehrten Flexibilisierung, ja geradezu eine Gleichzeitigkeit von Arbeitsformen und Arbeitsverhältnissen, und zwar in örtlicher, in zeitlicher und in betrieblicher/organisatorischer Hinsicht. Diese Veränderungen sind zwischenzeitlich bereits Gegenstand von politischen Vorstössen

zum Arbeitsrecht und insbesondere zu den Arbeitszeitvorschriften, welche in der aktuellen Form den Entwicklungen nicht ausreichend Rechnung tragen.

Die digitale Transformation führt zur Entwicklung neuer Geschäftsmodelle. Dabei können die Grenzen zwischen privaten und unternehmerischen Anbietern von Dienstleistungen und Produkten durchlässig werden (z.B. im Kontext von Beherbergungsplattformen). Ein gebräuchliches Stichwort lautet heute „Sharing Economy“, umschrieben als komplexes Ökosystem von Dienstleistungen auf Abruf sowie der über Online-Tauschplattformen laufenden vorübergehenden Nutzung von Gütern und/oder Dienstleistungen. Die wirtschaftliche Bedeutung der Sharing Economy ist in den letzten Jahren stark gestiegen.

6.2 Chancen und Risiken

SWOT-Analyse

Strengths	**Weaknesses**
• Rasche Entwicklung neuer Geschäftsmodelle möglich • Ausstrahlung über die Grenzen hinaus mit (relativ) geringem Aufwand • Oft niedrige Marktzutrittsschranken, wenn das Geschäftsmodell nicht stark datenbasiert ist • Aufhebung von zeitlichen und räumlichen Grenzen • Zugang zu globalen Ressourcen für Vorprodukte und Dienstleistungen • Zugang zu neuen Absatzkanälen • In der Regel hohe Verfügbarkeit allgemeiner und spezifischer Informationen (Big Data) • Viele neue Chancen durch raschen Wandel	• Abweichende Regelungen von bestehenden (analogen) Geschäftsmodellen • Erleichterter Angriff auf Marktstellungen, gerade auch aus dem Ausland • Strukturbrüche in Beschaffungs- und Verteilketten • Verletzlichkeit gegenüber Angriffen und Missbräuchen (Cybergefahren) • Hemmnisse für Datentransfer durch heterogene nationale Regulierungen • International nicht umfassend gewährleisteter Investitionsschutz • Reputationsrisiken wegen umfassender Transparenz und Information • Gleichzeitige Anwendbarkeit unterschiedlicher Regelungen (aufgrund extraterritorialer Anwendung) • Kurze „Halbwertszeit“ für spezifische Kenntnisse und Wissen (hohe Anforderungen an Weiterbildung, Forschung und Entwicklung)

Opportunities	Threats
• Nutzung von Chancen zur Deregulierung • Vergleichsweise niedrige Eintrittshürden (Chancen für Start-ups und KMU). • "First Mover Advantage" • Nutzung von Netzwerkeffekten • Erschliessung neuer Absatzkanäle • Möglichkeit von „Tailor made" Angeboten (Kleinserien) und Nutzen von Skaleneffekten, bei relativ niedrigen „sunk Costs" • Nutzen globaler Beschaffung („Outsourcing") • Weiterbildung und Entwicklung	• Kippeffekte und Monopolisierungen durch Netzwerkeffekte („winner takes it all"), insbes. bei Plattformen • Hohe Initialinvestitionen wegen globaler Ausrichtung der Angebote, namentlich für Marketing • Abhängigkeit von Plattformen aufgrund der Skaleneffekte • Unklarheiten mit Bezug auf Dateneigentum / Datennutzung („Datenpolitik") • Risiko, von der Technik abgehängt zu werden

Fazit:

Angesichts der raschen Entwicklung und neuer Marktstrukturen muss der Staat bestehende Lenkungsmassnahmen evaluieren und neue prüfen. Er hat dabei zu berücksichtigen, dass im digitalen Kontext die erwähnten Möglichkeiten und Chancen empfindlich auf Regulierungsmassnahmen reagieren. Da sie darauf beruhen, durch „Trial and Error" neue Wirtschaftsfelder zu erschliessen, kann eine voreilige und unbedachte Regulierung dazu führen, die Möglichkeiten neuer Geschäftsmodelle abzuwürgen, bevor sie überhaupt ein Profil entwickeln und wirtschaftlich Fuss fassen. Analoge und digitale Geschäftsfelder im gleichen Markt sind gleich zu behandeln und Marktverzerrungen zu vermeiden.

6.3 Regulatorischer Ordnungsrahmen und Handlungsbedarf

6.3.1 Vorbemerkungen

Angesichts der digitalen Transformation bedürfen überblicksmässig betrachtet drei Themen im B2B-Kontext der Diskussion; sie stehen auch im Herausforderungsbereich künftiger Regulierungen:

Im Bereich Sharing Economy hat sich die Expertengruppe darauf beschränkt, den allgemeinen Regelungsbedarf dieser neuen Geschäftsmodelle zu identifizieren (s. Ziff. 6.3.2). Der Daten- und Konsumentenschutz in der Sharing Economy wurde bereits im B2C Umfeld erörtert (Ziff. 5.3.2). Spezifische Rechtsbereiche der Sharing Economy wie das Arbeits-, Sozialversicherungs-, Steuer-, Mietrecht usw. werden nicht detailliert behandelt, da der Expertengruppe die entsprechende Expertise u.a. im Sozialversicherungs- und Steuerrecht fehlte. Da verschiedene Bundesämter im Auftrag des Bundesrates in diesem Bereich bereits Abklärungen an die Hand genommen hatten - u.a.

das SECO und das ASTRA - wollte die Expertengruppe auch keine Doppelspurigkeiten schaffen.

Im zweiten Abschnitt steht das Verhältnis der Unternehmen untereinander im Mittelpunkt. Wettbewerbs- und kartellrechtliche Fragen sind hier entscheidend (s. Ziff. 6.3.3).

Ziff. 6.3.4 geht auf das Thema der Schutzrechte bei der Datenbearbeitung und die Regelung des Datenflusses im B2B-Bereich ein und verweist auf Ziff. 7, in der der Zugang zu und die Besitzverhältnisse an Daten allgemein diskutiert wird.

Eine Reihe von weiteren bereichsübergreifenden Aspekten betrifft auch den B2B-Bereich. Um Wiederholungen zu vermeiden, wird an anderer Stelle diskutiert:

- Bedeutung einer allgemein gültigen elektronischen Identität (E-ID) für die Wirtschaft und Möglichkeiten der Umsetzung (s. Ziff. 4.4.6 und 8.4.2).
- Anpassung der Vorschriften zum Formerfordernis in Verträgen, weil die heutigen Anforderungen des Zertifizierungsdienstgesetzes zu kompliziert sind (s. Ziff. 5.3.2.3)
- Neue Haftungsfragen (s. Ziff. 7.3)
- Blockchain (s. Ziff. 9)

In allen potentiellen Handlungsfeldern ist die starke internationale Vernetzung im Auge zu behalten, ebenso die Tatsache, dass durch die Vernetzung in allen Bereichen, so namentlich im Wettbewerbsrecht wie auch im Datenschutzrecht, die extraterritorialen Effekte eine wachsende Rolle spielen. Insbesondere die Regulierungsbestrebungen in der EU sind deshalb im Auge zu behalten.

6.3.2 Regulierung bzw. Deregulierung aufgrund neuer Geschäftsmodelle in der Sharing Economy

Im Zusammenhang mit einer allfälligen Bewilligung und Überwachung bei neuen digitalen Geschäftsmodellen stellen sich Fragen des Abbaus bestehender Regulierungen sowie der Einführung von sich als notwendig erweisenden neuen Regulierungen. Die Beispiele für die Sharing Economy sind Vermittlungsplattformen wie vor allem die erfolgreichen Beherbergungsplattformen und Mobilitätsdienstleistungen; viele weitere Plattformen (z.B. für Car- oder Parkingsharing) bieten ihre Dienstleistungen an, haben aber noch nicht die gleiche Durchdringung erreicht. Auch dort werden mittel- bis langfristig Regulierungsfragen an die Hand zu nehmen sein.

6.3.2.1 Beherbergungsplattformen

Beherbergungsplattformen sind ein wichtiges neues Geschäftsmodell der Sharing Economy, das auch die Politik beschäftigt. Airbnb und andere Plattformen erleichtern die Suche nach Wohnraum, senken potenziell die Preise für die Nutzung der Wohnobjekte, bieten ein stärker diversifiziertes Beherbergungsangebot und erweitern die Chancen des Schweizer Tourismus dank der globalen Reichweite der Online-Angebote. Der Bundesrat hat sich bereits im „Bericht über die zentralen Rahmenbedingungen für die digitale Wirtschaft“ vom 11. Januar 2017 detailliert mit den Beherbergungsplattformen beschäftigt. Im Anschluss an das Postulat WAK-S 16.3625 „Überprüfung des Bundesrechts aufgrund der Entwicklung neuer Beherbergungsplattformen“ ist das WBF vom Bundesrat beauftragt worden, in einem Bericht bis spätestens Ende 2017

zu prüfen, ob in Anbetracht des vermehrten Auftretens von kurzfristigen und regelmässigen Untervermietungen via Plattformen eine Anpassung des Mietrechts angezeigt sei und ob die Nachbarn bzw. Mitglieder einer Eigentümergemeinschaft durch die heute gesetzlich eingeräumten Rechte ausreichend geschützt seien.

Gestützt auf eine extern eingeholte Studie „Regulierungen in der Beherbergungswirtschaft – Analyse der Deregulierungspotentiale auf Bundesebene aufgrund neuer internetbasierter Geschäftsmodelle“ hat der Bundesrat am 15. November 2017 den Bericht „Die Regulierung in der Beherbergungswirtschaft“ veröffentlicht. Die detaillierte Analyse gelangt zur Gesamtwürdigung, dass die meisten gesetzlichen Bestimmungen, die für die traditionellen Beherbergungsvermittlungen gelten, auch auf Online-Plattformen zur Anwendung kommen können. Mit Bezug auf verschiedene Gesetze (v.a. Raumplanungs-, Zweitwohnungs-, Ausländergrundstückerwerbs-, Behindertengleichstellungs-, Ausländer-, Lebensmittel-, direktes Bundessteuer-, Mehrwertsteuer-, Umweltschutz- sowie Radio- und Fernsehgesetz) wird im Lichte von bereits vorgenommenen Anpassungen kein Handlungsbedarf gesehen. Hinsichtlich des Arbeits- und Sozialversicherungsrechts erfolgt ein Verweis auf die parallelen (noch nicht abgeschlossenen) Arbeiten in der Bundesverwaltung. Die Rechte der Nachbarn und der Mitglieder einer Eigentümergemeinschaft erscheinen durch das Zivilgesetzbuch ausreichend geschützt. Im Mietrecht ergibt sich hingegen ein gesetzgeberischer Handlungsbedarf, und zwar mit Blick auf die Umschreibung des Begriffs der Ferienwohnung sowie insbesondere auf die Modalitäten der Zustimmung durch die Vermieterseite und die zulässigen Verweigerungsgründe. Diese Einschätzung ist sachgerecht und entspricht dem Grundsatz, nur dann regulatorisch tätig zu werden, wenn relevante Risiken eintreten könnten.

Zwei Themen sind jedoch abgesehen von den raumplanerischen Aspekten (Einhaltung/Durchsetzung der Zweitwohnungsinitiative) und wohnungspolitischen Bedenken (Mietzinserhöhungen zulasten der einheimischen Bevölkerung) zusätzlich im Auge zu behalten: Online-Beherbergungsplattformen sind global abrufbar und ermöglichen Vertragsabschlüsse zwischen beliebigen Vertragspartnern. Nicht zwingende Mietrechtsnormen finden deshalb zumindest für Geschäftsmieten keine Anwendung. Zur Verbesserung der Durchsetzung des geltenden Rechts wird im Bericht des Bundesrates sodann die Kooperation mit Online-Plattformen vorgeschlagen; dieses Vorgehen erscheint als sinnvoll, befreit aber nicht davon, künftig der Überprüfung der Einhaltung gesetzlicher Bestimmungen vermehrte Beachtung zu schenken.

6.3.2.2 **Mobilitätsdienstleistungen**

Die digitale Transformation bietet die Chance zu einem vernetzten Mobilitätsservice. Anknüpfungspunkt für eine solche Entwicklung ist der bereits bestehende Zusammenschluss einer Vielzahl von Mobilitätsdienstleistern des öffentlichen Verkehrs in der Schweiz. In Zukunft werden die Anbieter privater Serviceleistungen (Taxi, Mietautos etc.) und der Sharing Economy (Car-Sharing-Plattformen, Uber, etc.) diese bereits bestehenden Transportketten ergänzen – und künftige, völlig neue Marktteilnehmer wären ebenfalls zu berücksichtigen. Die Vorteile eines solchen ganzheitlichen Ansatzes liegen auf der Hand: ein massgeschneiderter Mobilitätsservice für den Kunden zu tieferen Kosten und eine effiziente Nutzung öffentlicher und privater Verkehrsmittel. Voraussetzung für eine solche Entwicklung ist ein dichtes und vernetztes Datennetz, das die Nutzer-, Geo-, Betriebs- und Preisdaten aller Marktteilnehmer zusammenführt. Eine solches existiert zurzeit nicht.

Vor diesem Hintergrund befürwortet die Expertengruppe das Projekt des Bundesrates, die Mobilitätsdienstleistungen weiter zu entwickeln und dafür die Verfügbarkeit von Grunddaten sicherzustellen.

In diesem Ökosystem wird die dafür notwendige Datendichte personen- und sachbezogener Daten (u.a. auch Betriebs- und Preisdaten) eine Herausforderung für den Datenschutz und eine austarierte Ausgestaltung des Datenflusses zwischen freier Verfügbarkeit und proprietärer Silohaltung bei den Dienstleistungsteilnehmern sein. Bei der Weiterentwicklung des Projekts Multimodale Mobilitätsdienstleistungen und Datenorganisation gilt es, diesem Umstand besonders Rechnung zu tragen. Ein weiterer Aspekt in diesem multimodalen System mit einer Vielzahl von (privaten) Anbietern ist mit Blick auf den Konsumentenschutz die Qualität der Dienstleistung, worunter insbesondere auch der wichtige „service après vente" fällt.

6.3.3 Verhältnis der wirtschaftenden Unternehmen untereinander

Unternehmen stehen miteinander im Wettbewerb, nicht nur in den traditionellen, sondern auch in den neuen (zum Teil erst im Entstehen begriffenen) digitalen Märkten (bzw. Online-Märkten). Auf die Tätigkeiten der wirtschaftenden Unternehmen gelangen insbesondere die folgenden zwei Gesetze zur Anwendung:

- Das Kartellgesetz (KG), das die erwünschte Quantität an Wettbewerb regelt (und nachfolgend genauer erläutert wird);
- Das UWG, das Bestimmungen zur Qualität des Wettbewerbs enthält; abgesehen von den Anordnungen, welche das Verhalten von Unternehmen gegenüber den Konsumenten regeln (s. Ziff. 5.3.2), ist zwischen den Unternehmen die Norm zur Übernahme eines marktreifen Arbeitsergebnisses (Art. 5 lit. c UWG) von Bedeutung, die eine Funktion des Investitionsschutzes beinhaltet und deshalb im Kontext der Diskussion der Eigentumsverhältnisse erläutert wird (s. Ziff. 7.2).

Der Bundesrat hat sich bereits im „Bericht über die zentralen Rahmenbedingungen für die digitale Wirtschaft“ vom 11. Januar 2017 mit dem kartellrechtlichen Handlungsbedarf beschäftigt und das SECO beauftragt, die Frage der Revision kartellrechtlicher Bestimmungen, insbesondere zur Fusionskontrolle, genauer zu analysieren. Der etwaige Handlungsbedarf als Folge der Digitalisierung ist vom SECO kombiniert worden mit fusionsrechtlichen Anliegen, die schon vor einigen Jahren im Rahmen einer umfassenden Revision des KG diskutiert worden sind, aber wegen anderer Gründe (z.B. der organisatorischen Ausgestaltung der WEKO) scheiterten, obwohl sie nicht eigentlich bestritten waren. Um Expertenmeinungen einzuholen, hat das SECO dann Swiss Economics beauftragt, einen wissenschaftlich fundierten Bericht zu verfassen.

Mit Datum vom 27. Oktober 2017 hat Swiss Economics den Bericht zum Thema „Einführung des SIEC-Tests“ vorgelegt, der aber vornehmlich das Thema der Fusionskontrolle, nicht die Digitalisierung diskutiert. Der SIEC-Test („Significant Impediment to Effective Competition“) wird schon lange in der EU angewendet und von den Kartellrechtsexperten auch für die Schweiz (ohne „Swiss Finish“) befürwortet. Die leichte Erhöhung der behördlichen Interventionsrate und der vertretbare Mehraufwand für die Behörden nach Einführung des SIEC-Tests erscheinen, wie der Bericht von Swiss Economics ausführt, als vertretbar. Diese Änderung des KG würde aber traditionelle Märkte und digitale Märkte gleichermassen betreffen. Entsprechende Überlegungen gelten auch für andere im Bericht von Swiss Economics angesprochene Themen, z.B. die Anpassung der Regel von Art. 9 Abs. 4 KG, welche die marktmächtigen Unternehmen ungeachtet der Aufgreifkriterien (Umsatzschwellen) verpflichtet, im Falle einer

Übernahme eine Meldung an die WEKO zu machen. Mit Blick auf die Digitalisierung hätte indessen die Frage geprüft werden sollen, ob der SIEC-Test, der auf Preisvariablen ausgerichtet ist, dafür überhaupt geeignet ist, weil in digitalen Geschäftsmodellen der Preis oft keine oder eine nur ganz untergeordnete Rolle spielt.

Der sich aus der Digitalisierung ergebende Handlungsbedarf ist im Bericht von Swiss Economics nicht vertieft angesprochen worden. Die Empfehlung, die Umsatzschwellen (Aufgreifkriterien) nicht zu senken, mag bei Einführung des SIEC-Tests vertretbar sein, selbst wenn dadurch weiterhin der Aufkauf kleinerer Unternehmen durch ein schon marktführendes Unternehmen nicht erfasst werden kann. Ob dieselben Überlegungen aber deckungsgleich für digitale Märkte gelten, bedürfte zumindest einer genaueren Begründung. Mit relativ kurzen Ausführungen lehnt es der Bericht von Swiss Economics auch ab, für digitale Märkte die Aufgreifkriterien um Transaktionswerte zu ergänzen, obwohl die Fusion von Facebook/WhatsApp gezeigt hat, dass der Zusammenschluss wegen der geringen Schwellenwerte von WhatsApp in den meisten Ländern nicht meldepflichtig war, und zwar ungeachtet des Transaktionswertes von ca. USD 19 Milliarden. Deutschland hat zwischenzeitlich eine Transaktionswertegrenze eingeführt (EUR 400 Mio.); in der EU wird über ein entsprechendes Projekt diskutiert. Auch in der Schweiz gehen die Kartellrechtsexperten mehrheitlich davon aus, dass bei Fusionen in digitalen Märkten eine „Kontrolllücke“ bestehe.

Das SECO muss dem Bundesrat bis Ende 2018 konkrete Vorschläge für eine KG-Revision unterbreiten. Unabhängig von einem Wechsel zum SIEC-Test erscheint es als angebracht, die aktuellen Aufgreifkriterien des KG mit Blick auf das Kriterium der Transaktionswerte in Übereinstimmung mit den internationalen Rechtsentwicklungen, die angesichts der globalen Reichweite digitaler Märkte massgeblich sind, zu überdenken.

In den letzten Monaten wird zudem ein weiteres Phänomen, das noch gar keinen Eingang in die Überlegungen der Bundesbehörden gefunden hat, vertieft diskutiert, nämlich das Problem der Wettbewerbsverfälschungen durch ähnlich konzipierte Algorithmen. Das Wettbewerbskomitee der OECD hat das Thema aufgenommen und beginnt, die einzelstaatlichen Wettbewerbsbehörden zu sensibilisieren. Materiell geht es um den Begriff der „abgestimmten Verhaltensweise“ bzw. der „Vereinbarung“, was nach heutigem Recht nur erfüllt wird, wenn die Wettbewerbsteilnehmer eine entsprechende Absicht haben. Gleichen sich aber Produkteangebote durch Algorithmen an, indem sie gegenseitig auf Preisveränderungen reagieren, fehlt diese (vom KG personal gedachte) „Absicht“ und es kommt zu einer vom KG nicht erfassten „Kollusion“ („tacit Collusion“). Die Thematik zwingt nicht zu vorschnellen regulatorischen Eingriffen, weil die offenen Formulierungen im KG auch neue Phänomene grundsätzlich zu erfassen vermögen, aber der Problematik ist mit Blick auf die anstehende KG-Revision doch die angemessene Beachtung zu schenken.

Empfehlungen:

18. Der Bund prüft im Kartellrecht, ob nicht alternativ zu den Umsatzschwellenwerten auch die Transaktionswerte geeignete Aufgreifkriterien bei der Prüfung von Unternehmenszusammenschlüssen wären.

19. Der Bund prüft unter Berücksichtigung der internationalen Entwicklungen, ob das Risiko einer durch Preisalgorithmen verursachten Kollusion im Kartellgesetz präziser geregelt werden soll.

6.3.4 Thema der Eigentumsverhältnisse bzw. Rechtsverhältnisse an Daten, soweit diese einen „Wert“ darstellen

Wichtige Aspekte dieses Themenbereichs sind die Analyse der Schutzrechte, heute vermittelt durch das Sachenrecht und das Immaterialgüterrecht, mit Auswirkungen auf die Übertragbarkeit von Daten bzw. Werten und auf den Investitionsschutz, unter Berücksichtigung der sich international abzeichnenden Entwicklungen. Eigentum und Werte haben eine zentrale Bedeutung für die Thematik „Datenbearbeitung und Informationssicherheit“.

Neben dem rechtlichen Eigentum, das Kontrolle ermöglicht, spielt die faktische Kontrolle durch Unternehmen, welche Daten in proprietären Datensilos aufbewahren, in der Praxis eine immer grössere Rolle. In dieser Situation stellt sich die Frage nach einem Zugang zu den Daten und nach der Datenportabilität (s. Ziff. 7.1).

6.3.5 Lauterkeits- bzw. Wettbewerbsrecht

Die allgemeinen Aufgreifnormen des UWG dürften mögliche lauterkeitswidrige Verhaltensweisen im digitalen Umfeld erfassen, weshalb sich eine Ergänzung des UWG nicht aufdrängt.

Profiling und personalisierte Daten unterlaufen die Schutzfunktion der PBV. Dynamisch-individuelle Preise erschweren die Transparenz und die Vergleichbarkeit von Preisen, womit der Nachfrager keine Möglichkeit zur Reaktion hat. Dennoch erweist sich eine allgemeine Regelung (z.B. im Vertragsrecht oder im UWG) nicht als zielführend; hingegen ist in Sektoren mit besonderem Schutzinteresse (Sozialschutz, Versicherungswesen/Krankenkasse etc.) die Einführung spezifischer Schutzregelungen zu prüfen.

6.3.6 Zugang zu Daten

Dem Aspekt „Zugang zu Daten“ kommt eine wichtige Bedeutung zu, weil die entsprechenden kartellrechtlichen Instrumente in der Praxis ungenügend greifen. In der Schweiz ist diese Diskussion, die Bestandteil einer umfassenden Datenpolitik (nicht nur der öffentlichen Hand bzw. der öffentlichen Unternehmen, sondern auch der privaten Unternehmen) sein müsste, noch kaum geführt worden. Einen Schritt weiter ist die EU-Kommission, die nicht an die bisher bestehenden Immaterialgüterrechte direkt anknüpfen, sondern ein eigenständiges Zugangsrecht entwickeln will, ähnlich dem Informationszugang gegenüber der öffentlichen Hand. Als B2C und B2B übergreifendes Thema werden die Fragen in Ziff. 7 vertieft.

7 B2C und B2B übergreifende Analysefelder: Datenzugang, Dateneigentum und neue Haftungsfragen

Zwischen einer proprietären Silohaltung und einem kompromisslosen freien Fluss der Daten liegt eine breite Palette verschiedener Möglichkeiten. Für die verschiedenen Datentypen einen austarierten Kompromiss zwischen freier Benutzung und beschränkter Weitergabe zu finden und eine zielführende rechtliche Erfassung der Daten zu definieren, ist die grosse Herausforderung für die Organisation der Datenbearbeitung. Kapitel 7.1 behandelt den Datenzugang und die Portabilität von Daten. Im Kapitel „Dateneigentum“ (Ziff. 7.2.) werden die Nachteile und die Vorteile möglicher Besitzverhältnisse an Daten und Alternativen dazu erörtert. Die Folgen der digitalen Transformation führen zu neuen Haftungsfragen. Diese sind Diskussionsgegenstand der Ziff. 7.3 „Neue Haftungsfragen“.

7.1 Datenzugang und Datenportabilität

7.1.1 Vorbemerkungen

Das Recht auf Zugang zu Daten betrifft den öffentlichen und den privaten Bereich. Wenn der „Inhaber“ der Daten nicht aktiv Transparenz schafft, stellt sich die Frage, ob passiv unter gewissen Umständen, insbesondere auf Begehren des Betroffenen hin, der Zugang zu Daten zu gewähren ist. Zudem ist zu klären, ob diejenigen Daten, zu denen der Zugang erwirkt worden ist, weiterverwendet werden dürfen.

Im öffentlichen Bereich sind gesetzliche Grundlagen zur Realisierung des Datenzugangs vorhanden, insbesondere das Öffentlichkeitsgesetz vom 17. Dezember 2004 (BGÖ) und die entsprechenden kantonalen Gesetze. Diese Rechtsakte umschreiben regelmässig die Voraussetzungen des Datenzugriffs sowie das anzuwendende Verfahren. Kein Regelungsgegenstand ist die Frage der Verwendung der Daten. Daneben haben sich in den letzten Jahren die Stimmen gemehrt, die für eine weiterreichende Transparenz der öffentlichen Daten eintreten: Ein zentrales Anliegen der Bewegung von Open Government Data (OGD) besteht im Zugang zu behördlichen Datenbeständen, um diese Daten hernach für eigene Zwecke verwenden zu können.

Die OGD-Thematik ist durch eine Interdepartementale Arbeitsgruppe unter der Führung des Schweizerischen Bundesarchivs analysiert worden; mögliche Vorgehensweisen betreffen die Anpassung der Spezialerlasse durch Gesetzgebungsprojekte der fachlich zuständigen Stellen, eine einheitliche Querschnittsregelung sowie die Anpassung der jeweiligen Spezialerlasse durch ein zentral geführtes Gesetzgebungsprojekt. Die Arbeiten sind indessen abgesehen von der Implementierung des OGD-Portals „opendata.swiss“ nicht weitergeführt worden. Nun hat das BAKOM indessen die Aufgabe, im Kontext des Berichts zur Datenpolitik auch Vorschläge zur OGD-Politik zu unterbreiten (s. auch Ziff. 8.5).

Im privaten Bereich beruhen die Datenzugangsrechte ebenfalls auf besonderen Bestimmungen; so kennen z.B. das Datenschutzrecht (Art. 8 DSG), das Auftragsrecht (Art. 400 OR), das Aktienrecht (Art. 697 OR) und viele andere Gesetze konkrete Auskunftsrechte des Betroffenen. In diesem Kapitel werden nur die Datenzugangsrechte im privaten Bereich thematisiert; zu prüfen ist, inwieweit die Schaffung solcher Rechte sinnvoll und zweckmässig ist.

7.1.2 Rechtfertigung von Zugangsrechten

Ähnlich wie bei der Beurteilung des Dateneigentums ist auch bei den Datenzugangsrechten zu differenzieren zwischen einer rechtlich abgesicherten Kontrolle und einer faktischen Kontrolle der Daten. Verfügt der Dateninhaber über eine ihm rechtlich zukommende Exklusivposition, z.B. gestützt auf ein Immaterialgüterrecht, ist er grundsätzlich berechtigt, Drittpersonen den Datenzugang zu verweigern. Allerdings gibt es selbst in solchen Situationen gewisse Beschränkungsgründe (z.B. die „fair Use"-Regelung im Urheberrecht), welche die Exklusivposition bis zu einem gewissen Grade abmildern.

Wichtiger in der Informationsgesellschaft ist die Einschränkung einer faktischen Datenkontrolle, die oft auf vorgenommen Datenverarbeitungen beruht; nimmt ein Unternehmen weitreichende Big Data Analysen vor, besteht die Tendenz, deren Resultate in proprietären Datensilos aufzubewahren und Drittpersonen nicht zur Kenntnis zu geben. Technische Gründe für eine Begrenzung des Datenzugangs lassen sich regelmässig nicht vorbringen. Von der Sache her geht es deshalb vielmehr darum, die technischen Rahmenbedingungen des Zugangs zu Personendaten und – nicht identisch – zu Sachdaten angemessen festzulegen. Zwei Konstellationen stehen im Kontext der Datenzugangsrechte im Vordergrund: der Zugang zu Daten aus Gründen des öffentlichen Interesses und der Zugang zu Daten eines Wettbewerbers.

1. Daten des öffentlichen Interesses sind insbesondere für die staatlichen Organe (z.B. Behörden) relevant. Der Gesetzgeber hat in dieser Situation festzulegen, unter welchen Voraussetzungen ein Datenzugangsrecht erwirkt werden kann. Weiter ist zu regeln, ob ein Entgelt für den Zugang zu den Daten geschuldet ist.
2. Komplexer ist die Situation mit Blick auf den Zugang zu Daten von Wettbewerbern. Der Grund liegt darin, dass viele Daten durch das Unternehmensgeheimnis geschützt sind; erhöhte Transparenz steht somit im Widerspruch zu Vertraulichkeitserwägungen. Ungeachtet von Geheimhaltungsvorschriften bleibt aber zu beachten, dass zum Teil der Zugang zu Daten erforderlich ist, um überhaupt den Marktzugang ins Auge fassen oder zumindest in einem vor- oder nachgelagerten Markt tätig werden zu können. Ein oft erwähntes Beispiel ist der Automobilmarkt; wenn der Garagist vom Automobilhersteller nicht gewisse Daten herausverlangen kann, wird unter Umständen die Reparatur nicht möglich sein. In einer solchen Situation ist eine Interessenabwägung im Rahmen der gesetzlichen Vorgaben vorzunehmen.

7.1.3 Rechtsinstrumentarium für den Datenzugang

Der Gesetzgeber hat die Möglichkeit, durch spezifische Normen einzelne Auskunftsrechte zu verankern. Wie erwähnt gibt es eine Vielzahl solcher Auskunftsrechte im schweizerischen Recht; querschnittsmässig im Vordergrund steht Art. 8 DSG, doch sind von dieser Bestimmung nur Personendaten betroffen. Ganz allgemein erscheint als nachteilig, dass es sich um punktuelle Regelungen handelt.

Die Verwendung von Daten durch Dritte lässt sich durch einen Lizenzvertrag regeln (Beispiel: Knowhow-Vertrag). Eine solche Lizenzerteilung erfolgt oft freiwillig, weil der Lizenzgeber daran interessiert ist, dass ein Dritter gegen Entgelt die Daten verwertet.

Der Gesetzgeber kann aber auch ein Regime von sog. Zwangslizenzen einführen. Diese regulatorische Intervention soll vermeiden, dass der Inhaber der faktischen Datenkontrolle sich weigert, freiwillig eine Lizenz einzuräumen. In einem solchen Fall sind die Voraussetzungen, unter denen eine Zwangslizenz erwirkt werden kann, gesetzgeberisch konkret festzulegen.

Ungeachtet der Tatsache, dass die EU seit 1996 einen Datenbankenschutz kennt, der zwar nicht sehr erfolgreich war, wie die Kommission selber eingesteht, schlägt die Kommission neue Rechtsinstrumente vor, nämlich ein Datenproduzentenrecht und ein Konzept für Daten-Zugangsrechte. Im Januar 2017 hat die Europäische Kommission im Dokument „EU Data Economy“ die Idee unterbreitet, die Einführung eines Systems mit Zwangslizenzen („compulsory Licences“) zu erwägen, teilweise auch als Alternative zur zurückhaltend beurteilten Einführung von Dateneigentum. In der Schweiz fehlen derzeit noch intensivere Überlegungen zum Konzept der Zwangslizenz.

Die Europäische Kommission äusserte sich bisher nur recht allgemein, d.h. nicht sehr detailliert, zu den Rahmenbedingungen des Regimes mit Zwangslizenzen; dessen Anwendung lässt sich in der Regel nur rechtfertigen, wenn im Markt spezifische Voraussetzungen gegeben sind. Regulatorisch festzulegen sind insbesondere die Aufgreifkriterien hinsichtlich der die Rechtsfolgen auslösenden faktischen Kontrolle von Daten. Querbezüge für die Beurteilung dieser Frage lassen sich insbesondere zum Wettbewerbsrecht herstellen; eine Vielzahl von Entscheiden des Europäischen Gerichtshofes (und auch einige Entscheide schweizerischer Gerichte) setzen die Leitplanken für den Zugang zu einer wesentlichen Einrichtung („essential Facility“). Ursprünglich hat die Rechtsprechung das als physische Installation verstanden, doch gilt zwischenzeitlich als anerkannt, dass auch Datenbestände eine wesentliche Einrichtung sein können (Entscheide Magill, IMS Health und Microsoft).

Wird daran gedacht, ein Regime mit Zwangslizenzen einzuführen, ist gesetzgeberisch weiter festzulegen, ob in horizontaler Weise eine allgemeine Regelung zu den Zwangslizenzen geschaffen werden soll, oder ob ein vertikaler, sektorspezifischer Regulierungsansatz vorteilhafter wäre. An sich spricht die notwendige Präzision der normativen Anordnungen für einen konkreten sektorspezifischen Ansatz, der es ermöglicht, die Besonderheiten des betroffenen Marktes in Betracht zu ziehen. Dieser Ansatz ist aber zeitaufwendiger und administrativ komplexer als eine allgemeine Regelung.

7.1.4 Bedingungen für Zwangslizenzen

Weil im Falle von Zwangslizenzen eine vertragliche Einigung über die Bedingungen des Datenzugangs und der Datenverwertung fehlt, sind gesetzgeberisch die wesentlichen Kriterien festzulegen. Als regulatorische Vorgaben für den Inhalt von Zwangslizenzen fallen folgende Aspekte in Betracht:

- Preisanordnungen: Daten stellen einen gewissen, wenn auch oft nur schwer feststellbaren Wert dar; die Wertquantifizierung ist, wie ein kürzlich publizierter OECD-Bericht festhält, ausgesprochen komplex. Doch darf diese Tatsache nicht davon befreien, den Versuch einer vernünftigen Quantifizierung einer Lizenzgebühr zu machen. Der Datenzugangsberechtigte hat keine Legitimation, die Daten ohne Bezahlung einer Lizenzgebühr zu verwenden.
- Das Datenvolumen, d.h. der Umfang der zugänglich zu machenden Daten, ist entweder freiwillig vertraglich oder durch eine regulatorische Vorgabe festzulegen. Ein Datenzugangsrecht kann nicht bedeuten, beliebig viele Daten zu erhalten, sondern „nur“ diejenigen Daten, die für den Betroffenen von Bedeutung sind.
- Der Lizenzvertrag oder die gesetzliche Regelung hat die Frage zu beantworten, ob der Berechtigte des Datenzugangsrechts die verfügbar gemachten Daten weiter verwerten darf oder nicht.
- Entsprechend den wettbewerbsrechtlichen Vorgaben darf das Datenzugangsrecht nicht mit weitergehenden Pflichten des Zugangsberechtigten gebündelt werden (sog. Koppelungsverbot).

Aus dem Immaterialgüterrecht ist das Rechtsinstrument der Zwangslizenzen schon seit vielen Jahren bekannt. In diesem Rechtsbereich hat sich auch die Erkenntnis durchgesetzt, dass die Lizenzbedingungen vertretbar sein müssen: Der entsprechende Test basiert auf sog. FRAND-Bedingungen (Fair, Reasonable and Non-Discriminatory). Zur Auslegung dieser FRAND-Eigenschaften gibt es bereits eine weitreichende Rechtsprechung, die auch im Kontext des Zugangs zu Daten nützlich sein kann.

Gesamthaft ist deshalb festzustellen, dass die Regelung von Zugangsrechten bei faktischer Datenkontrolle durchaus einen alternativen Ansatz zur Schaffung von Dateneigentum zu bieten vermag. Zwar lässt sich nicht übersehen, dass die Formulierung der gesetzgeberischen Vorgaben eines Zwangslizenzen-Regimes keine leichte, sondern eine komplexe Aufgabe ist; als Vorteil dieses Vorgehens fällt aber die Tatsache in die Waagschale, dass die geschilderten Probleme, welche durch die Schaffung von Dateneigentum verursacht würden, nicht eintreten.

Empfehlung:

20. Der Bund prüft die Ausgestaltung eines Zwangslizenzen-Systems mit Blick auf den Zugang zu Sachdaten.

7.1.5 Datenportabilität an Personen- und Sachdaten

7.1.5.1 Datenportabilität an Personendaten

Im Kontext der Diskussionen zum Dateneigentum und zum Datenzugang wird oft auch der Aspekt der Datenportabilität thematisiert. Inhaltlich geht es darum, dass die an den Daten berechtigte Person vom Unternehmen, das faktisch die Kontrolle über die Daten ausübt, verlangen kann, dass die Daten an ein anderes Unternehmen „übergeben“ (transferiert) werden. Dies setzt auch voraus, dass die Daten in einer gebräuchlichen und maschinenlesbaren Form vorliegen.

Mit Blick auf die Personendaten hat die DSGVO in Art. 20 ein Recht auf Datenportabilität verankert. Zusätzlich zur DSGVO hat Frankreich auf nationaler Ebene ebenfalls ein Recht auf Datenportabilität eingeführt, das parallel seit Ende Mai 2018 in Kraft steht; ein Vorbehalt gilt, wenn der Datenbearbeiter durch seine Tätigkeiten eine wesentliche Wertsteigerung der Daten bewirkt hat. Soweit bekannt gibt es keine weiteren Länder ausserhalb des DSGVO-Bereichs, die ein Recht auf Datenportabilität kennen.

In den Erläuterungen des Vorentwurfs zum E-DSG hat der Bundesrat zum Ausdruck gebracht, dass die Einführung eines Rechts auf Datenportabilität nicht beabsichtigt sei. In der Vernehmlassung ist an diesem Positionsbezug nicht unerheblich Kritik geübt worden. In der Botschaft zum E-DSG hat der Bundesrat jedoch an seiner Auffassung festgehalten mit der Begründung, dass die Datenportabilität mehr darauf abziele, den Wettbewerb zu verstärken als die Persönlichkeit zu schützen. Ebenfalls wird darauf verwiesen, dass die so verlangte Aufbereitung von Daten in eine maschinenlesbare und strukturierte Form gerade für kleinere Unternehmen sehr kostenintensiv wäre.

In vielerlei Hinsicht stellt die Datenportabilität eine Chance zum Paradigmenwechsel bei der Bearbeitung von Personendaten dar. Die Portabilität eröffnet dem Datensubjekt die Chance, standardisiert und automatisiert Daten, die es selber betreffen, aus den Silos der bisherigen Datenbearbeiter herauszulösen und selbst zu verwalten. Da dies schwierig ist, wird auf sogenannte Personal Information Management-Systeme (PIMS) zurückgegriffen. Das bisherige „Datenobjekt“ erhält so die Chance, als Subjekt über

seine Daten im Sinne einer ausgeübten informationellen Selbstbestimmung zu bestimmen und Daten zu monetarisieren. Gleichzeitig würde dies den freien Fluss von Personendaten fördern und könnte mit der Zeit zu einem geregelten Markt für Personendaten führen, weil der Preis für Daten spürbar wird. Davon würden die Datensubjekte, die Forschung, die Wirtschaft und letztlich die gesamte Gesellschaft profitieren.

Vor diesem Hintergrund vertritt die Expertengruppe die Ansicht, dass der freie Fluss von Personendaten im Sinne der informationellen Selbstbestimmung zu fördern sei und dass das Datenschutzrecht als Anknüpfungspunkt für ein Portabilitätsrecht dienen könne. Alternative Rechtsinstrumente für die Umsetzung einer Datenportabilität wie etwa das Kartellrecht mit einem wettbewerbsgestützten Ansatz scheinen weniger geeignet, da die Durchsetzung wettbewerbsrechtlicher Ansprüche langwierig und teuer ist. Andere Gesetze wie dasjenige zum elektronischen Patientendossier sind zu sektoriell und decken im genannten Fall nur Patientendaten ab.

Anders als in der DSGVO soll das bestehende Auskunftsrecht im DSG als Ausgangspunkt für die Entwicklung einer Datenportabilität dienen. Damit wären nicht nur wie in der DSGVO die vom Nutzer direkt übergebenen, sondern alle bearbeiteten Daten (auch die beobachteten) abgedeckt. Die Erweiterung des Auskunftsrechts müsste weiter das Recht des Datensubjekts auf eine Datenherausgabe in einer standardisierten und maschinenlesbaren Form konkretisieren und sicherstellen, damit auch die direkte Übertragung an Dritte (z.B. PIMS, s. ausführlicher in Ziff. 7.1.5.2) möglich wird.

Ein erweitertes Auskunftsrecht führt, sofern die Daten gespeichert worden sind, auch zu Interessenkonflikten zwischen Datenbearbeitern, Personen und Dritten, u.a. wenn es um Geheimhaltung geht. Diese Konflikte müssen geprüft werden und zwecks Ausgleichs als Einschränkungen in das erweiterte Auskunftsrecht einfliessen. Vorbereitende Arbeiten wurden bereits an die Hand genommen: Am 9. Mai 2018 hat der Bundesrat das Bundesamt für Justiz mit einer Analyse des Regelungsbedarfs zu einer sektor- bzw. branchenspezifischen Einführung der Portabilität von Personendaten beauftragt.

7.1.5.2 „Sharing the Wealth"-Prinzip

Dieser ökonomische Ansatz zielt darauf ab, neben den Datenbearbeitern auch die Betroffenen zu Nutzniessern der neuen Wertschöpfung durch Daten zu machen. Das „Sharing the Wealth"-Prinzip würde die betroffenen Personen zu gleichberechtigten Partnern aufwerten, die den Wertzuwachs der Daten erkennen könnten. Die Betroffenen hätten auch Klarheit darüber, wie ihre Daten gesammelt und genutzt werden, was die bisherige Wissensasymmetrie abbauen würde. Bereits 2016 hat der Europäische Data Protection Supervisor sogenannte PIMS als wertvolle Möglichkeit erkannt, den Benutzern die Kontrolle über ihre Daten zurückzugeben – er sieht diesen Ansatz aber eher als Ergänzung zur DSGVO und dem Prinzip der Portabilität denn als Alternative.[12] Weiter wäre zu überlegen, wie Anreize für den Datenbearbeiter gesetzt werden könnten, die bisherige Exklusivität der Datenbearbeitungskontrolle aufzugeben. Die Beteiligung würde zwangsläufig zu einer Ökonomisierung der Daten führen, verbunden mit Vorteilen, aber auch Nachteilen wie dem ungelösten Problem der Eigentumsrechte an Daten.

[12] https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_de [Stand 30. April 2018].

Empfehlung:

21. Der Bund ergänzt unter Berücksichtigung der internationalen Entwicklungen das Datenschutzrecht um das Element der Datenportabilität.

7.1.5.3 Portabilität an Sachdaten

Bei den Sachdaten kann sich die Frage der Portabilität ebenfalls stellen. Ein Unternehmen, das seine Datenaufbewahrung in einer Cloud vornimmt, ist unter Umständen interessiert, die Datenaufbewahrung neu durch einen anderen Cloud-Anbieter vornehmen zu lassen. Meist wird im unternehmerischen Kontext eine solche Datenportabilität mit Kündigungsvorschriften und Anordnungen zur Datenweiterleitung vertraglich geregelt.

Mit einem Vorschlag für eine neue Verordnung zum freien (grenzüberschreitenden) Fluss der Sachdaten innerhalb der EU-Länder hat die Europäische Kommission am 13. September 2017 die Thematik aufgenommen [COM (2017) 495 final]. Art. 6 des Entwurfs sieht eine Bestimmung zu „Porting of Data“ vor. Angeordnet wird aber nicht ein zwingendes Recht auf Portabilität von Sachdaten, sondern die Kommission will die Industrie ermutigen, Verhaltensrichtlinien zu entwickeln, welche den Wechsel von Internetanbietern erleichtern sollen. Die Diskussion dieses Vorschlags bleibt abzuwarten. Die Schweiz hat bisher keine Aktivitäten in diese Richtung unternommen. Allfällige Vorstösse in Richtung einer Portabilität an Sachdaten müssen die internationalen Entwicklungen berücksichtigen und ein „Swissfinish“ vermeiden.

Empfehlung:

22. Der Bund prüft unter Berücksichtigung der internationalen Entwicklungen eine Regelung der Portabilität von Sachdaten.

7.2 Dateneigentum

Das Schlagwort „Dateneigentum“ wird im Recht und in der Politik sehr oft, aber unterschiedlich verwendet und hat bisher keine klaren Konturen erhalten. Seine begriffliche Erfassung ist auch nicht einfach, weil sich verschiedenste Datenkategorien und Formen von Dateninhaberschaft in Betracht ziehen lassen.

7.2.1 Begriffliche Auslegeordnung

Wenn von „Dateneigentum“ gesprochen wird, sind zwei Begriffselemente zu umschreiben, nämlich die „Daten“ und das „Eigentum“. Die Rechte aus dem Eigentum sind im Gesetz, wenn auch ohne konkrete Definition, umschrieben; der Bezug auf das Sacheigentum ist aber offensichtlich (Art. 641 und Art. 713 ZGB). Im Kontext der Daten steht indessen oft die „Inhaberschaft“ im Vordergrund.

Komplexer ist die Umschreibung des Begriffs der Daten. Eine für das Recht wesentliche grundsätzliche Zweiteilung unterscheidet zwischen Personendaten und Sachdaten. Die Personendaten haben einen Bezug zum Persönlichkeitsrecht, das – ähnlich wie das Eigentum – ein absolutes und gegenüber jedermann durchsetzbares Recht vermittelt. Die Personendaten werden regelmässig durch die Datenschutzgesetzgebung erfasst. Bei den Sachdaten stehen wirtschaftliche Elemente stärker im Vordergrund; die Zuordnung an bestimmte Personen oder Unternehmen erlaubt die Bearbeitung und Verwertung der Daten.

Die Daten sind vom Begriff der „Information“ zu trennen: Die syntaktische Dimension betrifft in der digitalen Welt die Struktur der Daten (Sequenzen von 0 und 1), die semantische Dimension bezieht sich auf das Verhältnis verschiedener Daten untereinander und führt letztlich zur Information, d.h. zum hinter den Daten stehenden Inhalt. Die pragmatische Dimension fragt danach, ob das durch die Information vermittelte Wissen bestimmte Wirkungen hat oder ein gewisses Ziel erreicht. Eigentum an der syntaktischen Struktur der Daten hat infrastrukturelle (nicht inhaltliche) Auswirkungen; Eigentum an einer Information kann zwar wertvoll sein, doch stellt sich auch hier das Problem der Monopolisierung der Information.

Weiter lässt sich differenzieren zwischen den „freiwilligen Daten“ (dem bewussten Austausch von Daten zwischen verschiedenen Personen), den „beobachteten Daten“ (die von Drittpersonen gesammelt werden, aber für einen Datenaustausch zur Verfügung stehen), sowie den „abgeleiteten Daten“ (die sich aus grösseren Datenanalysen etwa mittels Big Data Analysen ergeben).

Ungeachtet der Frage, welcher Datenbegriff verwendet wird, ist zwischen der rechtlichen und der faktischen Kontrolle der Daten zu unterscheiden: Die rechtliche Zuordnung basiert auf einem bestimmten Rechtstitel und vermittelt ausschliessliche Rechte an Daten mit Blick auf deren Gebrauch und deren Verfügung. Die faktische Kontrolle bezieht sich auf die Möglichkeit, den Zugang zu den Daten bzw. Informationen zu kontrollieren, d.h. die Zugänglichmachung zu regulieren, was zu einer „eigentumsähnlichen Macht“ zu führen vermag.

7.2.2 Rechtfertigung für die Schaffung von Dateneigentum

Die Schaffung eines neuen Rechtsinstituts durch den Gesetzgeber ist gerechtfertigt, wenn die Analyse der bestehenden Rechtslage zur Erkenntnis führt, dass ein Handlungsbedarf besteht. Sowohl theoretische Anforderungen als auch praktische Bedürfnisse vermögen eine gesetzgeberische Initiative zu begründen.

Als Rechtfertigung für regulatorische Interventionen wird meist auf das Vorliegen von Marktversagen hingewiesen. Diese Situation tritt ein, wenn der Markt die erwünschten Güter oder Dienstleistungen nicht produziert. Konkret müsste also die Schaffung, die Bereitstellung und der Gebrauch von Daten unterbleiben, obwohl die Gesellschaft an diesen Vorgängen ein Interesse hätte, d.h. es müssten trotz der problemlosen Duplizierbarkeit von Daten die Anreize fehlen, um die Datenwirtschaft zu beleben. Eine solche Situation ist in der praktischen Realität nicht festzustellen: Der exponentielle Anstieg des Datenvolumens lässt vermuten, dass grosse Anreize bestehen, Daten zu schaffen und auch auszutauschen.

Als weiterer Grund für eine Regulierung kommen die Transaktionskosten in Frage, in der digitalen Welt also insbesondere die Such- und die Verhandlungskosten. Bisherige Untersuchungen haben indessen gezeigt, dass aller Voraussicht nach die Transaktionskosten nicht erheblich sinken würden, wenn der Gesetzgeber ein Dateneigentum einführen würde. Standardisierungseffekte treten zudem oft wegen Betroffeneninteressen „freiwillig“ ein.

Ökonomisch könnte auch die Fehlallokation von Kosten und Vorteilen als Begründung für eine Regulierung dienen. Zwar wird zum Teil darauf hingewiesen, dass die faktischen Dateninhaber aus Datensammlungen wirtschaftliche Vorteile generieren können, ohne die eigentlichen Subjekte der Daten dafür entschädigen zu müssen (sog. Aspekt der Internalisierung von Gewinnen). Untersuchungen scheinen zu belegen, dass die Wertrealisierung für die Datensubjekte nicht nur schwierig wäre, sondern der

jährliche Ertrag, der persönlich erwirtschaftet werden könnte, wahrscheinlich gering sein dürfte (wohl weniger als CHF 100.- pro Jahr).

Die ethischen Werte, etwa die Freiheit, die Würde und die Autonomie des Menschen, die Nichtdiskriminierung, das informationelle Selbstbestimmungsrecht oder die Befähigung zur Selbstentfaltung lassen sich besser durch Grundrechte oder nicht-wirtschaftliche Regulierungen verwirklichen als durch die Einführung eines Dateneigentums. Auch das Problem der rechtlichen Unsicherheit mit Bezug auf die Berechtigung an Daten erscheint als nicht so gravierend, dass ein neues Rechtsinstitut eingeführt werden müsste. Hingegen bestehen gewisse Regelungslücken, die sich aus dem Fehlen von Dateneigentum ergeben und die einer besonderen Berücksichtigung bedürfen (vgl. Ziff. 7.2.6).

7.2.3 Rechtliche Anknüpfungspunkte für Dateneigentum

Vom Wortlaut her scheint das Dateneigentum dem Sacheigentum ähnlich zu sein. Das Zivilgesetzbuch konkretisiert den Begriff des Eigentums anhand der körperlichen Sache und der Naturkräfte (Art. 641 und Art. 713 ZGB). Daten sind aber grundsätzlich nicht physischer Natur und erfüllen damit – nach weitgehend einhelliger Auffassung – das konstituierende Charaktermerkmal des Sacheigentums nicht. Ein subjektives Ausschliesslichkeitsrecht an Daten lässt sich deshalb nicht ohne weiteres bejahen. Der Gesetzgeber müsste die sachenrechtlichen Normen erweitern: Rechtstechnisch wäre dies durch eine nicht sehr komplizierte Gesetzesanpassung möglich. In diesem Sinne hat die EU-Kommission in einem Diskussionspapier vom Januar 2017 die Schaffung von Dateneigentum zur Diskussion gestellt. Nicht auszuschliessen wäre aber, dass eine solche Regulierung unvorhersehbare neue Probleme verursachen würde (Ziff. 7.2.5).

Ähnliche Überlegungen gelten für das Besitzrecht (Art. 919 ZGB); wie beim Eigentum ist auch beim Besitz die physische Eigenschaft vorausgesetzt (tatsächliche Gewalt über eine Sache). Der Begriff „Datenbesitz“, der oft verwendet wird, ist somit rechtlich nicht verankert.

Seit über 100 Jahren sind die Immaterialgüterrechte ein fester Bestandteil der Rechtsordnung. Im Gegensatz zum Sacheigentum bedarf es z.B. im Patent- und im Urheberrecht keiner physischen Formgebung, was der virtuellen Gestalt eines Dateneigentums entgegenkommen würde. Die Problematik der Immaterialgüterrechte besteht aber darin, dass die Daten regelmässig die gesetzlich erforderliche Erfindungshöhe bzw. die geistige Schöpfung nicht aufweisen. Vereinzelt wird zwar versucht, ein Immaterialgüterrecht sui generis zu begründen, doch hat sich dieser Ansatz bisher nicht durchgesetzt.

Neben den klassischen Immaterialgüterrechten haben sich in den letzten Jahrzehnten auch Sonderformen von ähnlichen Rechtspositionen entwickelt, etwa die sog. Nachbarschaftsrechte (bzw. die Leistungsschutzrechte) oder der Rechtsschutz sui generis von Datenbank-Inhabern. Dieses in der EU verankerte Schutzrecht sui generis hat die Schweiz bewusst nicht übernommen, ebenso wie z.B. die USA. Der konzeptionelle Schutzgedanke der erwähnten Rechtspositionen, der auf „flüchtige“ künstlerische Ausdrucksformen bzw. auf Datensammlungen (nicht Daten) abzielt, ist aber mit einem Dateneigentum nicht vergleichbar, d.h. eine analoge Anwendung des Immaterialgüterrechts erweist sich als nicht sachgerecht.

Schliesslich lässt sich Dateneigentum durch Vertrag oder Delikt begründen; diese Rechtspositionen weisen aber nicht eine absolute, sondern nur eine relative (schuldrechtliche) Wirkung auf. Handlungsunrecht, beruhend auf dem Deliktsrecht oder dem

Wettbewerbsrecht, liegt z.B. bei einem Verstoss gegen den Schutz von Fabrikations- und Geschäftsgeheimnissen oder gegen das Verbot der Übernahme fremder Arbeitsergebnisse vor; ein weitergehender Schutz von Daten ist dem Recht hingegen nicht bekannt.

Die Schwierigkeiten, ein Rechtsinstitut für das „Dateneigentum“ zu finden, führen – ähnlich wie bei der Beurteilung der Rechtfertigungsgründe – zur Erkenntnis, dass es sinnvoller ist, die eigentlichen Regulierungslücken zu identifizieren (Ziff. 7.2.6). Der Vollständigkeit halber ist vorerst aber noch die Frage zu prüfen, ob die Schaffung von Dateneigentum nicht neue Probleme verursachen würde (Ziff. 7.2.5).

7.2.4 Daten als Entgelt

Ein eigentlicher Paradigmenwechsel hat in letzter Zeit insoweit stattgefunden, als Daten nicht nur (gegen Entgelt) verkauft und erworben werden, sondern dass Daten auch als Entgelt für Sachlieferungen und Dienstleistungen Verwendung finden können. Die Möglichkeit, Daten als Entgelt für den Erwerb anderer Güter einzusetzen, führt zu neuen Rechtsfragen, die sich mit den heutigen Gesetzen kaum sachgerecht beantworten lassen.

Diesen Paradigmenwechsel nimmt der erwähnte EU-Richtlinienvorschlag (COM 2015 634 final) zu den digitalen Vertragsinhalten auf und regelt die Daten (auch) als „Währung der Zukunft“. Konkret lässt sich zwischen den Vertragsparteien vereinbaren, dass der Anbieter von Sach- oder Dienstleistungen mit der Zurverfügungstellung von Daten des Kunden „entschädigt“ wird. Wenn also der Kunde die Sach- oder Dienstleistung nicht traditionell mit Geld bezahlt, dafür aber die Verwendung seiner Daten durch den Anbieter erlaubt, handelt es sich nicht um ein „unentgeltliches Geschäft“, sondern die Vereinbarung beruht auf der Annahme, dass die Daten des Kunden für den Anbieter einen wirtschaftlichen Wert haben, welcher einer Geldleistung entspricht.

Eine Sonderanordnung hat sich zudem als notwendig erwiesen für den Fall, dass der Vertrag erfolgreich angefochten worden ist (z.B. wegen Grundlagenirrtums oder gravierender Sachmängel), mit der Folge, dass wegen Wandelung die gegenseitigen Leistungen rückabzuwickeln sind. In einer solchen Situation ist der Anbieter verpflichtet, die ihm vom Kunden zur Verfügung gestellten Daten in einem technisch üblichen und standardisierten Format wieder zurück zu übertragen, ohne zuvor die Daten zu kopieren und ohne sie in anderweitiger Form zu verwenden. Die Regelung entspricht dem Gedanken der Datenportabilität, wie sie bereits in Art. 20 DSGVO vorgesehen ist. Dass kein identischer Wortlaut gewählt wurde, ist rechtstechnisch nicht ganz unproblematisch, doch soll eine entsprechende Anpassung des Richtlinienentwurfs in der Endfassung noch erfolgen.

Mit der Verabschiedung der Richtlinie ist im 2. Halbjahr 2018 zu rechnen. Die Schweiz kennt keine entsprechenden Rechtsgrundlagen. Nicht zuletzt im Zusammenhang mit den Fragen zum Dateneigentum sowie zum Zugang zu Daten ist aber die Frage zu prüfen, ob nicht eine ähnliche Regulierung ins Auge gefasst werden sollte.

7.2.5 Neue Probleme nach Einführung von Dateneigentum

Mit gesetzgeberischen Aktivitäten lassen sich erkannte Regelungslücken, die durch neue Entwicklungen verursacht worden sind, schliessen. Solche Vorschriften wirken sich indessen dann negativ aus, wenn dadurch bisher nicht vorhandene Probleme im rechtlichen Umfeld entstehen.

7.2.5.1 Ungewissheitsfaktoren

Wie die letzten Jahre gezeigt haben, wandelt sich das technologische Umfeld sehr schnell. Flächendeckende starre Rechtsregeln riskieren, die technologische Entwicklung zu behindern. Insbesondere zeigt die Erfahrung, dass die Entstehung von Rechtsnormen oft so lange dauert, dass sich der technologische Zustand zwischenzeitlich bereits verändert hat. Neue oder hochspezialisierte Technologien könnten deshalb trotz der Einführung von Dateneigentum in einen rechtsfreien Raum fallen.

Nach den bisherigen empirischen Untersuchungen scheint das Fehlen von Dateneigentum keinen negativen Einfluss auf die Investitionen und Innovationen zu haben. Genauer zu untersuchen wäre aber gleichzeitig, ob die Einführung von Dateneigentum nicht neue wirtschaftliche Belastungen hervorrufen würde, die gravierender wären als der Nichtbestand eines absoluten Rechts. Insbesondere könnten bei Bestehen von Dateneigentum gewisse Transaktionskosten im Falle eines Eigentümerwechsels entstehen.

Die Ungewissheiten in rechtlicher Hinsicht betreffen den Umfang eines allgemein umschriebenen Dateneigentumsrechts. Der Spielraum für die Gerichte in der Ermessensausübung dürfte relativ breit sein, was sich widersprechende Urteile zur Folge haben könnte.

7.2.5.2 Probleme der Implementierung

Die grössten Herausforderungen im Falle der Schaffung von Dateneigentum dürften sich im Kontext der Implementierung eines neuen Rechtsinstituts ergeben. Ein Dateneigentumsregister, ähnlich dem Grundbuch oder dem Handelsregister, scheint keine ideale Lösung zu sein, weil dies hohe Administrationskosten nach sich ziehen könnte. Die Blockchain-Technologie würde sich als Infrastruktur zwar grundsätzlich für Registrierungszwecke eignen; die Blockchain liegt aber in der Hand von Privaten und damit ausserhalb einer klaren Kontrollsituation (vgl. Ziff. 9.1.3). Der Staat ist grundsätzlich kein Beteiligter dieser Infrastruktur. Aus diesem Grunde ist die Durchsetzung von Rechten durch obrigkeitliche Vorkehren zumindest stark erschwert. Die Festlegung des Eigentums ist aber eine unumgängliche Anforderung, um dessen Durchsetzung auch praktikabel und effizient zu gestalten.

Datenmärkte sind, wie die Erfahrung zeigt, einem erhöhten Monopolisierungsrisiko ausgesetzt; gutes Anschauungsmaterial bieten die Verfahren der EU gegen Google, die eine unzulässige Monopolisierung einzelner Märkte diagnostizierten und vorläufig mit der Ausfällung erheblicher Bussen endeten. Die Schaffung von Dateneigentum würde weitere absolute Rechte begründen und könnte damit Monopolisierungstendenzen fördern.

Weiter stellt sich die Frage, ob das Dateneigentum tatsächlich ewig bestehen oder ein „Verfallsdatum“ haben sollte, weil Daten weniger ausgeprägt als Sachen nicht unbedingt für die Ewigkeit gedacht sind. Technisch lässt sich ein Verfallsdatum zwar programmieren; ob der Code aber regelmässig die sachgerechten Löschungssignale enthält, bleibt zumindest ungewiss.

7.2.6 Potentieller Handlungsbedarf wegen des Fehlens von Dateneigentum

Eine Rechtfertigung für die Schaffung von Dateneigentum wäre dann gegeben, wenn Regelungslücken im heutigen Recht zu Rechtsunsicherheiten führen würden und der Erlass von Normen einen Beitrag zur Rechtsbeständigkeit zu leisten vermöchte.

7.2.6.1 Mögliche Regelungslücken

Nachfolgend werden einige Beispiele (ausgenommen das Steuerrecht, das in diesem Bericht nicht thematisiert wird) diskutiert, die nach der heute gegebenen Rechtslage als nicht befriedigend geregelt erachtet werden:

- Erbrechtliche Fragen: Das traditionelle Erbrecht basiert mit Bezug auf den Übergang der Erbschaftswerte an die berechtigten Erben auf der Annahme, dass die Erbmasse aus Sacheigentum und Forderungen besteht. Unklar ist hingegen, ob z.B. Daten des Verstorbenen, die z.B. auf Facebook gespeichert sind, herausverlangt werden können. Dieser Problematik ist gesetzgeberisch Beachtung zu schenken. Der E-DSG (Art. 16) enthält nun eine ausdrückliche Bestimmung, welche mit Bezug auf Personendaten anordnet, unter welchen Bedingungen die Erben in die Daten des Verstorbenen Einsicht nehmen oder deren Löschung beantragen können.
- Datenportabilität: Weil Daten oft einen wirtschaftlichen und/oder sozialen Wert haben, muss der Berechtigte in der Lage sein, diese Daten von einem Internet-Intermediären auf einen anderen Intermediär zu übertragen. Art. 20 der DSGVO sieht nun mit Bezug auf Personendaten ein Recht auf Datenportabilität vor. Der E-DSG enthält keine entsprechende Bestimmung (Botschaft, S. 43), doch soll die Problematik noch genauer analysiert werden.
- Eine gewisse Rolle spielt die Datenportabilität auch für Sachdaten. Eine Regelung dazu lässt sich im Kontext des Datenzugangs erwägen (s. Ziff. 7.1.3).
- Konkurs: Fällt ein Unternehmen, welches die Daten speichert, in Konkurs, muss grundsätzlich eine Aussonderung zugunsten der die Daten betreffenden Person möglich sein. Das heutige Konkursrecht ist auf die Aussonderung von Sacheigentum und die Abtretung von Forderungen ausgerichtet (Art. 242 SchKG); kein Regelungsgegenstand sind virtuelle Daten. Eine Aussonderung würde voraussetzen, dass ein sehr weiter Begriff des Gewahrsams mit Bezug auf Daten zur Anwendung käme. Eine geringfügige Gesetzesanpassung erscheint deshalb als sinnvoller. Die Arbeitsgruppe zu den Kryptowährungen beabsichtigt, bis Ende 2018 einen Regelungsvorschlag zu unterbreiten.
- Verlust von Geräten/Daten: Der Verlust von Geräten (z.B. iPhone, iPad) bedeutet eine gewisse wirtschaftliche Werteinbusse, die angesichts der Anschaffungswerte solcher Geräte heute aber nicht mehr allzu stark ins Gewicht fällt. Das Schweizer Recht stellt die notwendigen Instrumente bei Verlust von Daten durch die Einwirkung durch Dritte zur Verfügung: Diebstahl, Entzug und Verrat sind abgedeckt. Das Problem liegt aber bei der Durchsetzung. So ist es aufgrund der beliebigen Kopierbarkeit von Daten für den Kläger schwierig, den Sachverhalt gegenüber den Strafverfolgungsbehörden entsprechend darzulegen, wenn es um unrechtmässig erlangte Daten durch unbeteiligte Dritte geht. Bei Verlust von nicht personenbezogenen Daten ohne Einwirkung durch Dritte ist das heutige Recht nicht vorbereitet. Straf- oder lauterkeitsrechtliche Anknüpfungspunkte fehlen. Es stellt sich die Frage, ob hier ein besserer Schutz für den Dateninhaber nötig ist. Diese Tatsache bedeutet aber nicht zwingend, dass ein allgemeines Dateneigentum zu schaffen ist, sondern genauer analysiert werden muss, welcher Regelungsansatz dieses Problem lösen kann.
- „Web (Screen) Scraping": Die Gewinnung von Informationen durch gezieltes Extrahieren der gewünschten Daten (z.B. mittels Crawler) von fremden Webseiten ist ein weiteres, bisher ungenügend beachtetes Problem. Diese Thematik betrifft

aber eher den Aspekt des Verhaltens im Wettbewerb als die sachenrechtliche Zuordnung von Daten.

Einzelne Konstellationen rechtfertigen somit gesetzgeberische Aktivitäten. Die folgende Übersicht zeigt, inwiefern bisherige Rechtsinstitute mit den entsprechenden Ergänzungen ein Datensachenrecht für Personen- und Sachdaten ersetzen können:

Positive Seite der Eigentumsherrschaft (Verfügungsrechte)	**Personendaten**	**Sachdaten**
Besitz an der Sache	• Informationelle Selbstbestimmung (nur beschränkte Wirkung) • Erbrecht: Spezifische Norm im E-DSG • Konkursrecht: Ungeklärte Rechtslage	• Immaterialgüterrechte (IGR), z.B. PatG und URG, wenn Voraussetzungen erfüllt (Erfindungshöhe, geistige Schöpfung) • Knowhow Schutz (stärker in EU als in CH) • Schutz vor Datenbankinhabern (in EU, wenn auch umstritten, nicht in CH, nur Art. 5 lit. c UWG) • Idee und Information an sich nicht geschützt • Konkursrecht: Ungeklärte Rechtslage
Gebrauch der Sache	• Informationelle Selbstbestimmung (nur beschränkte Wirkung) • Besitzesrecht (nur beschränkte Wirkung)	• Immaterialgüterrechte (IGR), z.B. PatG und URG, wenn Voraussetzungen erfüllt (Erfindungshöhe, geistige Schöpfung) • Knowhow Schutz (stärker in EU als in CH) • Schutz vor Datenbankinhabern (in EU, wenn zwar umstritten, nicht in CH) • Idee und Information an sich nicht geschützt
Verfügung über die Sache	Datenübertragung: • Kauf- oder Lizenzvertrag • Datenportabilität (Art. 20 DSGVO, nicht in E-DSG)	Datenübertragung: • Kauf- oder Lizenzvertrag, soweit Immaterialgüterrecht gegeben

	Verlust der Daten: nicht geregelt	• Datenportabilität gemäss Art. 6 EU-Verordnung (COM 2017 495 final) Verlust der Daten: nicht geregelt

Negative Seite der Eigentumsherrschaft (Abwehrrechte)	**Personendaten**	**Sachdaten**
Herausverlangen der Sache	Auskunftsrecht des DSG	Datenzugangsrechte: in Entwurf der EU-Verordnung (10. Januar 2017, COM(2017) endg., 9, 12 ff.) vorgesehen, in der Schweiz noch offen
Abwehr von Beeinträchtigungen	Persönlichkeitsschutz des ZGB Persönlichkeitsschutz des E-DSG Vorbehalt: (Widerufbare) Einwilligung des Betroffenen	Ggf. UWG-Schutz

Fazit:

Wie in Ziff. 7.2.6.1 erläutert, bedarf es im Fall des erwünschten Verzichts auf die Schaffung eines besonderen Dateneigentums der Anpassung einzelner Gesetze, um im Bereich der digitalen Datenbearbeitung spezifische Regelungslücken zu schliessen und Rechtssicherheit herbeizuführen.

Bei Daten im Konkurs ist im SchKG eine Norm zu schaffen, welche die Aussonderung von Daten ermöglicht (ähnlich wie bei anderen materiellen Vermögenswerten).

Im ZGB oder DSG ist das Recht der Erben, an die Daten des Verstorbenen zu gelangen, zu regeln.

Die Datenportabilität lässt sich, soweit gerechtfertigt, im Kontext des Auskunftsrechts vorsehen. Vor der Einführung weiterer Regelungen sind die internationalen Entwicklungen zu verfolgen.

7.2.6.2 Regulatorische Grundsatzentscheidung

Die vorerwähnten Beispiele zeigen, dass im gegenwärtigen Zeitpunkt das Fehlen von Dateneigentum in der Schweizer Rechtsordnung zu gewissen Regelungslücken führt, weil die traditionellen Rechtsinstitute den virtuellen Charakter der Daten nicht ausreichend erfassen. Die angesprochenen Beispiele zwingen aber nicht zur grossflächigen Schaffung von Dateneigentum als neuem Rechtsinstitut; absolute Rechte könnten zwar in bestimmten Konstellationen mehr Rechtssicherheit bringen, lösen aber die sich stellenden Probleme nicht vollumfänglich.

Vielmehr ist zu prüfen, ob im Sinne der vorerwähnten Überlegungen nicht punktuelle und spezifische Gesetzesanpassungen den erwünschten Rechtsschutz schaffen könnten, ohne gleichzeitig die erwähnten unerwünschten Folgeprobleme zu verursachen. Dem Gesetzgeber kommt dabei ein recht grosses Entscheidungsermessen zu.

Empfehlung:

23. Der Bund schliesst Lücken betreffend die Rechte der Betroffenen beim Rechtsschutz, insbesondere durch Anpassungen des Bundesgesetzes über Schuldbetreibung und Konkurs und des Erbrechts.

7.3 Neue Haftungsfragen

7.3.1 Digitale Herausforderungen für das Haftungsrecht

Das Internet of Things (IoT) als neue, auf dem Internet aufgebaute Netzwerkstruktur ist ursprünglich für den Geschäftsverkehr konzipiert worden, erfasst aber mehr und mehr auch private Belange. Von grosser praktischer Bedeutung ist insoweit der Gesundheitssektor, der besonders datenintensiv, aber auch datensensitiv ist. Eine im IoT auftretende Fehlfunktion (z.B. wegen eines Design- oder Konstruktionsfehlers oder einer Manipulation) kann doppelte (negative) Konsequenzen haben:

- Die Fehlfunktion führt ggf. zu Datenverlusten oder zur widerrechtlichen Offenlegung von Daten; rechtlich steht dabei die Einhaltung des Datenschutz- und des Datensicherheitsrechts zur Diskussion.
- Die Fehlfunktion vermag zu physischen Schäden zu führen, etwa zur Explosion angeschlossener Geräte oder zur Beeinträchtigung von Drittprodukten (z.B. Verderben von Lebensmitteln im ausser Betrieb gesetzten Kühlschrank).

Die Vielzahl der (Markt-) Beteiligten in den IoT-Netzstrukturen erschwert angesichts der oft vorhandenen Abhängigkeiten das Auffinden des bzw. der Verantwortlichen. Beim explodierenden Kühlschrank kann es z.B. der Gerätehersteller, der Netzwerkbetreiber, der Entwickler des Softwareprogramms oder der sich falsch verhaltende Kunde sein.

Autonome Systeme
Noch komplexer sind die Haftungsprobleme bei den sogenannten autonomen Systemen, z.B. beim Einsatz von Industrierobotern, Medizinrobotern, selbstfahrenden Autos oder Drohnen. Die Charakteristik der autonomen Systeme besteht darin, dass sie in der Lage sind, die Umgebung selbstständig zu „analysieren“ und zu „interpretieren“ sowie gestützt darauf potenziell sachgerecht zu agieren oder zu reagieren.

Die traditionellen Haftungsregeln beruhen auf dem Prinzip, dass jemand eine „Kontrolle“ auszuüben vermag, etwa mit Bezug auf das eigene Verhalten, auf produzierte und angebotene Produkte oder auf spezifische Tätigkeitsentfaltungen. Diese traditionelle „Kontrollfunktion“ lässt sich bei autonomen Systemen oft nicht leicht zuordnen. Bei einem selbstfahrenden Auto könnte dessen Produzent, der Bestandteilzulieferer oder der Entwickler eines der vielen eingesetzten Softwareprogramme für die Fehlfunktion verantwortlich sein.

Die meisten Rechtsordnungen kennen zwar die sogenannten Gefährdungshaftungen; wer einen „gefährlichen“ Zustand schafft oder betreibt, unterliegt der Verantwortung, Vorsichtsmassnahmen zu ergreifen, um Schädigungen zu vermeiden. Im Vergleich zu einem Atomkraftwerk oder einem Fahrzeug ist beim Roboter die Gefährdungslage weniger klar.

Informationssicherheitssensitive Märkte
Die Informationssicherheit spielt nicht nur beim Internet of Things und bei den autonomen Systemen eine grosse Rolle, sondern ganz allgemein, wenn Daten bearbeitet und übermittelt werden. Die Komplexität der Informationssicherheitsanforderungen ergibt sich daraus, dass Produkte und Dienstleistungen die verschiedensten Datenebenen betreffen, z.B. die Sammlung und Bearbeitung von Daten, die Softwareentwicklung (in Produkte integriert oder nicht), die Anwendungsebene (z.B. Vielzahl von Apps) sowie die Sensoren und Aktoren. Bereits heute zeigen sich die Herausforderungen der Haftungszuordnung z.B. im Kontext des Cloud-Computing oder des Outsourcing. Überdies ist zu berücksichtigen, dass die eigentlichen gesetzlichen Grundlagen nicht sehr stark entwickelt sind. Vielmehr beruhen die Anforderungen an die Informationssicherheit zu weiten Teilen auf mannigfaltigen Selbstregulierungen der Branchenverbände; der Vorteil solcher Regulierungen besteht in der Technologieorientierung und der Flexibilität, doch ist deren Verbindlichkeit bzw. Durchsetzbarkeit nicht immer gewährleistet (Beispiele: ISO IEC 27000f, BSI Grundschutz Kompendium, usw.).

7.3.2 Schwächen des heutigen Haftungsrechts

Überblicksmässig betrachtet kennen die meisten Haftungsordnungen der europäischen Länder vier Grundtypen von Haftungsarten, nämlich die Vertragshaftung, die Deliktshaftung, die Gefährdungshaftungen und die besonderen Spezialhaftungen.

7.3.3 Vertragshaftung

Die Vertragshaftung ist Regelungsgegenstand des Vertragsrechts. Die Defizite der geltenden Haftungsregeln sind heute teilweise anerkannt, etwa mit Bezug auf die Umschreibung der Konformität digitaler Vertragsinhalte; die EU will deshalb diesbezüglich tätig werden.

Auch die Smart Contracts stellen mit Bezug auf die Ausgestaltung von Rechtsbehelfen neue Herausforderungen. Weil Intermediäre auf Blockchain fehlen, muss der (selbstausführende) Programmcode im Falle einer Abweichung vom Vertragsprogramm eine

vorbestimmte Lösung (bzw. einen Konfliktmechanismus) vorsehen. Über eine technologische Schnittstelle, welche die Blockchain mit der realen Welt verbindet (oft "Oracle" bzw. "Orakel" genannt) lässt sich auch die Mitwirkung einer Schlichtungsstelle vorsehen (s. Ziff. 9.3.5 lit. a).

Die steigende Bedeutung der Ausgestaltung der Vertragssprache im Programmcode führt überdies zu einer Verwischung von Vertrags- und Delikts- bzw. Produktehaftung. Zwar besteht zwischen dem Nutzer und dem Anbieter eines virtuellen Gutes eine Vertragsbeziehung, doch erstreckt sich diese nicht zwingend auf den Entwickler des Programmcodes (je nach vertraglicher Ausgestaltung), womit dem Nutzer im Falle einer Fehlfunktion nur ausservertragliche Ansprüche verbleiben.

7.3.4 Deliktshaftung

Die Deliktshaftung (Art. 41 OR) kommt im Falle der widerrechtlichen Verursachung eines voraussehbaren Schadens, gestützt auf ein absichtliches oder fahrlässiges Verhalten zum Zuge. Regelmässig vorausgesetzt ist die Verletzung einer (standardisierten) Sorgfaltspflicht.

Eine grundsätzliche Problematik im hochtechnologischen Kontext besteht in der Tatsache, dass für den Anbieter eines Produktes oder einer Dienstleistung oft nur schwer abschätzbar ist, welche Dritte durch eine Fehlfunktion geschädigt werden könnten. Die Einschätzung des Risikobereichs gestützt auf die übliche Sorgfaltspflicht erweist sich somit als sehr komplex. Diese Beurteilung trifft für IoT-Produkte und autonome Systeme gleichermassen zu.

Umgekehrt vermag der Anbieter eines IoT-Produktes oder eines autonomen Systems oft auch nicht abzuschätzen, welchen Einfluss die Einzelbestandteile, die von Dritten bereitgestellt worden sind, auf die Lieferung haben. Vertraglich wird zudem die Haftung für von Dritten gelieferte Einzelbestandteile oft wegbedungen, was zur Folge hat, dass der geschädigte Benutzer lediglich über einen ausservertraglichen Haftungsanspruch verfügt, der ihm die ganze Beweislast bei der Durchsetzung von Ersatzansprüchen auferlegt.

7.3.5 Gefährdungshaftungen

7.3.5.1 Produktehaftung

Gestützt auf die Richtlinie 85/347/EWG kennen die Länder der EU seit den späten 80er Jahren gesetzliche Vorgaben zur Produktehaftung. Die Schweiz ist mit dem Produktehaftpflichtgesetz vom 18. Juni 1993 (PrHG) gefolgt. Bei der Produktehaftung handelt es sich um eine verschuldensunabhängige Kausalhaftung.

Die Problematik des Produktehaftungsrechts für datenbasierte Produkte und Dienstleistungen liegt in der Tatsache, dass dort grundsätzlich nur von physischen Gütern verursachte Schäden erfasst sind. Als Produkte gelten bewegliche Sachen und Elektrizität (Art. 3 PrHG). Virtuelle Güter (z.B. Daten) fallen somit nicht in den Anwendungsbereich des Produktehaftungsrechts. Jedenfalls im kommerziellen Bereich geht es bei den IoT-Geschäften zwar meist um physische Güterlieferungen, doch verursachen in der Regel nicht diese Güter einen Schaden, sondern die integrierte Software für die Lieferkette oder die Bearbeitung bzw. Auswertung der zugrundeliegenden Daten. Diese Elemente sind indessen nicht physisch und deshalb kein Produkt. Ähnliche

Überlegungen gelten für autonome Systeme, wie etwa das Beispiel des selbstfahrenden Autos zeigt; ein Unfall dürfte vielfach eher auf einen „Datenfehler“ oder einen Softwarefehler als auf einen Konstruktionsfehler beim Auto zurückzuführen sein.

Bei virtuellen Gütern ist es überdies schwierig, den traditionellen Begriff des „Mangels“ zu konkretisieren. Gemäss Art. 4 PrHG ist ein Produkt fehlerhaft, wenn es nicht die Sicherheit bietet, die man unter Berücksichtigung aller Umstände zu erwarten berechtigt ist. Abgesehen davon, dass in der Realität oft nicht immer völlig klar ist, mit welchen Sicherheitsstandards ein Benutzer rechnet, mag auch der Nachweis der vorhandenen Kausalkette, die zum „Mangel“ führt, nur schwierig zu erbringen sein.

Dass die „traditionelle“ Produktehaftung im Lichte der neuen technologischen Entwicklungen einer Anpassung bedarf, hat die EU erkannt. Am 25. April 2018 hat die Kommission detaillierte Vernehmlassungsergebnisse zur Anpassung der Richtlinie 85/347 publiziert. Ähnliche Überlegungen müsste sich auch der Schweizer Gesetzgeber machen.

7.3.5.2 Produktesicherheitshaftung

Erst einige Jahre nach dem Erlass der Produktesicherheits-Richtlinie 2001/95/EU hat die Schweiz diese Thematik mit dem Bundesgesetz vom 12. Juni 2009 über die Produktesicherheit (PrSG) angegangen. Gemäss dessen Art. 2 handelt es sich bei einem Produkt um eine verwendungsbereite bewegliche Sache, was bedeutet, dass virtuelle Güter wie bei der Produktehaftung nicht erfasst sind.

Weil die Bestimmungen des Produktesicherheitsrechts insbesondere für autonome Systeme nicht mehr als vollumfänglich sachgerecht erscheinen, stellt sich die Frage, ob durch analoge Anwendung dieser Vorschriften im neuen technologischen Kontext sinnvolle Lösungen erreicht werden können, oder ob eine Gesetzesanpassung in Betracht zu ziehen ist.

7.3.5.3 Fazit

Produktehaftung und Produktesicherheitshaftung sind nicht für den Kontext virtueller Güter angelegt. Die Gründe dafür sind die Virtualität des Produkts (Daten), fehlende Standards für die Beurteilung des „Mangels“ am Produkt und schwer zu rekonstruierende Kausalketten. Ebenfalls erscheinen Elemente der Produktesicherheitshaftung angesichts von KI und autonomen Systemen nicht mehr als sachgerecht.

7.3.6 Spezialhaftungen

7.3.6.1 Providerhaftung

Die E-Commerce-Richtlinie 2000/31/EG enthält besondere Haftungsregeln zuhanden der Internet Provider (Art. 12-15). Die Haftungsregelung ist abgestuft nach dem Ausmass, in welchem der Internet Provider in die inhaltliche Ausgestaltung der durch ihn angebotenen Informationen involviert ist; je mehr sich der Internet Provider nur auf die technische Abwicklung der elektronischen Kommunikationen beschränkt, desto tiefer ist das Haftungsniveau.

Die Schweiz kennt keine entsprechenden Regeln. Im sehr detaillierten Bericht des Bundesrates zur zivilrechtlichen Verantwortlichkeit von Providern vom 11. Dezember

2015 wird kein dringender allgemeiner Handlungsbedarf diagnostiziert, was im Schrifttum teilweise anders beurteilt wird. Immerhin bestehen konkretisierende Selbstregulierungen der Branche.

7.3.6.2 Datenschutzhaftung

Mit der neuen DSGVO und dem bevorstehenden DSG kommt es zu einer starken Ausweitung der Pflichten von Datenbearbeitern jeglicher Art. Überwiegend handelt es sich zwar um aufsichtsrechtlich relevante Datenschutzpflichten. Im Falle einer Verletzung sind aber auch die Grundlagen für eine erleichterte Durchsetzung zivilrechtlicher Ansprüche gelegt.

Konkret beruht in diesem Fall die zivilrechtliche Haftung auf Vertrag oder Delikt. Der Vorteil des Aufsichtsrechts besteht aber darin, dass der Aspekt der Widerrechtlichkeit in einem amtlichen Verfahren geprüft wird und hernach der Geltendmachung von Ansprüchen in einem Zivilverfahren zugrunde gelegt werden kann. Die Zahl solcher Verfahren dürfte künftig deshalb steigen. Ein spezifischer Regelungsbedarf abgesehen vom Erlass des DSG lässt sich indessen nicht diagnostizieren.

7.3.6.3 Netzwerkinfrastrukturhaftung

Im Jahre 2016 hat die EU die „Network and Information Security (NIS)"-Richtlinie (2016/1148/EU) erlassen. Diese bis 2018 umzusetzende Richtlinie sieht vor, dass eine ganze Reihe von Massnahmen zu treffen ist, welche die Sicherheit der Netz-werkinfrastrukturen verbessern, und zwar sowohl mit Blick auf Störungsanfälligkeiten als auch mit Blick auf Attacken verschiedenster Art durch Dritte (Cybersicherheit). Zwar sind die ursprünglich vorgeschlagenen Vorgaben der EU-Kommission in der Endfassung teilweise etwas abgeschwächt worden, doch ist nach Verankerung der Grundsätze im nationalen Recht doch mit einem verbesserten Cybersicherheitsniveau zu rechnen.

Die fernmelderechtlichen Rahmenbedingungen in der Schweiz gehen wesentlich weniger weit als die „NIS"-Richtlinie; aus diesem Grunde stellt sich für den Gesetzgeber die Frage, inwieweit die Grundsätze im schweizerischen Recht autonom nachzuvollziehen sind (s. 8.2.3.1).

7.3.7 Neue Haftungskonzepte

Mit einer Kommunikation und einem ausführlichen Staff Working Paper vom Januar 2017 schlägt die EU vor, neue Haftungskonzepte zu diskutieren und ggf. später zu implementieren. Im Vordergrund stehen drei Themen, nämlich Sorgfaltspflichten und Verantwortlichkeitszuordnung, Risikomanagement-Modelle und freiwillige oder zwingende Versicherungslösungen.

7.3.7.1 Sorgfaltspflichten und Verantwortlichkeitszuordnung

Schon heute besteht, insbesondere angesichts der durch die Deliktshaftung bewirkten Herausforderungen, eine Pflicht, Strategien zu entwickeln und Massnahmen umzusetzen, welche die Informationssicherheitsrisiken in Unternehmen sowie in den Geschäftsbeziehungen mit Dritten minimieren. Die entsprechenden Aufgaben werden von den Unternehmen auch in einem mehr oder weniger weitgehenden Umfang bereits heute wahrgenommen. Das Stichwort lautet „Enterprise Risk Management"; neben technischen Präventionsmassnahmen kommt der Schulung und Sensibilisierung der Mitarbeiter eine immer grössere Bedeutung zu.

Zu den relevanten Faktoren der Risikominimierung gehören auch selbstregulatorische Vorgaben mit Bezug auf die Benutzung von elektronischen Hilfsmitteln (z.B. iPhone, iPad, usw.). Die getroffenen Massnahmen können einen Einfluss auf die Beurteilung der Risikoallokation bei Auftreten eines Schadensfalls haben; die Implementierung der präventiven Vorkehren wirkt sich somit letztlich risikomindernd für die Unternehmen aus.

7.3.7.2 Risikomanagement-Modelle

Über die Sorgfaltspflichten und die Verantwortlichkeitszuordnung hinaus schlägt die EU vor, eigentliche Vorgaben zu Risikomanagement-Modellen einzuführen; je nach Grösse des verursachten Informationssicherheitsrisikos ist von den Anbietern von Gütern und Dienstleistungen ein unterschiedliches Ausmass an Risikovermeidungs- und Risikominimierungsmassnahmen zu verwirklichen.

Bei der Allokation der entsprechenden Aufgaben denkt die EU daran, das von der Ökonomie schon vor Jahrzehnten entwickelte Konzept des „cheapest Cost Avoider" zu realisieren. Die Vornahme von Massnahmen zur Vermeidung von Informationssicherheitsrisiken ist also demjenigen aufzuerlegen, welcher die niedrigsten Kosten für deren Vornahme hat; betroffen sein kann auch der Benutzer, falls es für ihn leicht ist, einen Beitrag zur Informationssicherheit zu leisten.

7.3.7.3 Freiwillige und zwingende Versicherungslösungen

Eine weitere, wohl alternative Massnahme, die von der EU in Betracht gezogen wird, liegt in der Einführung einer Versicherungslösung, die freiwillig oder verpflichtend sein kann. Das Ziel einer solchen Lösung liegt darin, denjenigen Beteiligten (v.a. den Endabnehmern von Produkten) eine Entschädigung zukommen zu lassen, die einen (grösseren) Schaden erlitten haben, ohne dass eine Ersatzleistung durch den Haftpflichtigen erfolgt, entweder, weil der Schädiger angesichts der Komplexität der wirtschaftlichen Beziehungen kaum gefunden werden kann, oder weil der Geschädigte seinen Beweispflichten angesichts der gegebenen Umstände nicht nachzukommen vermag. Ob eine solche Versicherungslösung in der nun laufenden Vernehmlassung eine ausreichende Anerkennung findet, lässt sich im Moment noch nicht abschätzen. Jedenfalls bedürfte eine Weiterverfolgung dieses Ansatzes noch vertiefter technischer und wirtschaftlicher Abklärungen.

7.3.7.4 Ausblick

Am 25. April 2018 hat die Europäische Kommission eine Reihe von Dokumenten publiziert, welche als Diskussionsgrundlage für die künftige Ausgestaltung von rechtlichen Bestimmungen zum freien Fluss der Daten, aber auch zur Haftung mit Blick auf die künstliche Intelligenz dienen sollen. Konkrete Massnahmen, ausser die stärkere Beachtung ethischer Prinzipien, werden nicht vorgeschlagen. Welche konkrete Haftungsordnung im Sinne der vorerwähnten Modelle zur Realisierung gelangt, steht deshalb im Moment noch nicht fest.

Empfehlung:

24. Der Bund prüft unter Berücksichtigung der internationalen Entwicklungen, insbesondere derjenigen in der EU, den Handlungsbedarf im ausservertraglichen Haftungsrecht (Produktehaftung, Produktesicherheit, Providerhaftung, Netzwerkinfrastrukturhaftung) und die allfällige Einführung neuer Haftungskonzepte.

8 Analysefeld Government to Citizen/Business (G2Ci/B)

8.1 Einführung

Schutzaufgaben des Staates

Staatliche Akteure haben den Cyberraum als Operationssphäre entdeckt. In der Folge sind die Datenbearbeitung und die Informationssicherheit einem zunehmenden Risiko ausgesetzt.

Es muss davon ausgegangen werden, dass zukünftige militärische Konflikte hybrid ausgetragen werden und Cybermittel auf allen Ebenen offensiv zur Anwendung gelangen werden. Dazu gehören auch Desinformationskampagnen. Aufgrund von Zeit- und Ressourcenmangel hat die Expertengruppe beschlossen, auf eine Vertiefung dieses spezifischen Szenarios zu verzichten. Sie verweist diesbezüglich auf den Sicherheitspolitischen Bericht 2017 und die entsprechenden Analysen der Armee im Bereich Cyber Defense.

Ebenso stellen die staatlichen Aktivitäten im Cyberraum (Spionage und Sabotage) eine zunehmende Herausforderung dar, wie, ab welcher Eskalationsstufe und in welchem Umfang der Staat auch im Sinne von Art. 2 der Bundesverfassung Schutzaufgaben für die Gesellschaft übernehmen muss. Zu nennen ist die nachrichtendienstliche Ausspähung, die Instrumentalisierung von IKT-Firmen sowie das Dossier „Safe Harbor“ und das Nachfolgekonstrukt „Privacy Shield“. Schliesslich wird die digitale Transformation zunehmend von organisierter Cyberkriminalität gefährdet. Dabei verwischen sich die Grenzen zwischen staatlichen, staatsnahen und nichtstaatlichen Akteuren mit kriminellen Zielen zusehends.

Da der Cyberraum als erweiterter öffentlicher und privater Raum wahrgenommen wird, stellt sich die Frage, wie der Staat dort seine Aufgaben (Schutz von Freiheit und Sicherheit, Chancengleichheit, Wohlfahrt, friedliche und gerechte Ordnung) erfüllen kann.

Die Ausgestaltung der Schutzpflichten und Möglichkeiten des Staates gegenüber der Gesellschaft durch den Eingriff in die Privatsphäre des Einzelnen ist ein weiterer Schlüsselaspekt von G2Ci. Während der Erstellung des Berichts waren im Bereich der schweizerischen Staatssicherheit die Überwachung des Post- und Fernmeldeverkehrs – Bereich des Bundesgesetzes vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) – und das neue Nachrichtendienstgesetz vom 25. September 2015 (NDG) die bestimmenden Themen. Zentral war die Diskussion, wie stark die Privatsphäre des einzelnen Individuums zum Vorteil der ganzen Gesellschaft eingeschränkt werden darf. Da diese Frage weder direkt mit der zukünftigen technologischen Entwicklung noch mit der Datenbearbeitung in Verbindung steht, sondern vielmehr Entscheide im Bereich der Sicherheitspolitik erfordert, verzichtete die Expertengruppe auf eine Vertiefung. Hingewiesen wird jedoch auf das Missbrauchspotenzial von Technologien und Macht.

Staat als Dienstleister (E-Government) und Förderer einer Open Government Data- und einer Open Data Kultur

Der Staat ist gefordert, die Grundversorgung der Gesellschaft mit einem sicheren, leistungsfähigen und stabilen Datenzugang zu ermöglichen (z.B. mittels Breitbandnetz), ohne den eine moderne Datenbearbeitung und eine digitale Gesellschaft nicht möglich sind. Im Verhältnis G2Ci geht es auch um den Staat als Anbieter behördlicher Leistungen in digitaler Form (E-Government) und dazugehörende Basisdienstleistungen wie die elektronische Identität (E-ID).

Enorme Datenmengen werden gesammelt und immer weiter zentralisiert. Die Kontrolle über diese Datenmengen liegt heute aber nicht bei der öffentlichen Forschung oder beim Staat, sondern zunehmend bei Privaten und zwar vor allem bei den Gatekeepern zum Internet: Google, Apple, Facebook, Amazon (auch GAFA genannt), und Alipay/Alibaba. Obwohl Eigentum und Besitz von Daten bisher rechtlich nicht eindeutig geklärt sind, werden Daten heute überwiegend proprietär behandelt und liegen in entsprechenden firmeneigenen Silos. Diese Daten stehen einerseits einer unabhängigen und öffentlichen Forschung und damit der Gesellschaft nicht zur Verfügung, sondern nur noch privaten, wirtschaftsgetriebenen Interessenkreisen. Andererseits bringt die Situation Entwicklungs- und Wettbewerbsvorteile für die Unternehmen: Sie werden kompetitiver und versprechen den Konsumentinnen und Konsumenten sowie den Nutzern mehr Nutzen und Komfort. Die aktuelle Diskussion rund um die digitale Entwicklung der Wirtschaft zeigt aber auch, dass sich solche Datensilos innovationshemmend auswirken können.

Umso mehr ist eine neue Balance zugunsten einer Open Data Entwicklung zu finden, bei der die einzelnen Interessen der Gesellschaft, der Wirtschaft und bundesnaher Betriebe gegeneinander abgewogen werden. Im privatrechtlichen Bereich werden der Datenzugang und das Problem der offenen Datenflüsse in Ziff. 7.1 erörtert. Der Zugang zu Behördendaten und Daten bundesnaher Stellen wird folgend im Kapitel Open Government Data (s. Ziff. 8.5) behandelt. Schliesslich wird der Frage nachgegangen, ob das bestehende BGÖ die Informationspflicht des Staates gegenüber den Bürgerinnen und Bürgern erfüllt.

Staat und Demokratie 2.0

Die digitale Transformation verändert die Daten- und Informationsflüsse. Für die Demokratie birgt das Chancen durch die Möglichkeit einer unmittelbareren Partizipation und einer besseren Information der Bürgerinnen und Bürger. Hingegen birgt dies auch Risiken: Digitale Technologien ermöglichen wie noch nie zuvor eine personenbezogene Massenmanipulation. Verfälschte, einseitige, nicht überprüfte und nicht überprüfbare Informationen einerseits und die Informationsflut andererseits erschweren es den Bürgerinnen und Bürgern, sich eine möglichst qualifizierte Meinung zu bilden und unbeeinflusst Entscheide zu fällen. Die Situation der Medien und ihre Zukunft als vierte Macht im Staat spielt dabei eine wichtige Rolle.

8.2 Schutzaufgaben des Staates

8.2.1 Ist-Zustand, weitere Entwicklung, Chancen und Risiken

Wesentlicher Bestandteil der digitalen Souveränität ist der Anspruch, den Cyberraum zu kontrollieren und innerhalb dieser Grenzen Staatsorgane, Sicherheit, Landesrecht

sowie alle Gesellschaftsteilnehmerinnen und -teilnehmer, ihre Selbstbestimmung, Menschenwürde und Werte zu schützen. Die nicht an Territorien gebundene Struktur des Internets und dessen Grundidee der Offenheit erschweren aber die Durchsetzung dieser hoheitlichen Prinzipien. Es ist im Internet relativ einfach, den freien Datenverkehr zu blockieren. Autoritäre Staaten haben zu diesen Mitteln gegriffen, um den Informationsaustausch unter ihre Kontrolle zu bringen. Weitaus schwieriger ist es, den Datenfluss mit dem Ziel höherer Sicherheit zu bewerkstelligen, ohne dabei die Informations- und Entfaltungsmöglichkeiten der Bürgerinnen und Bürger einzuschränken; denn jede präventive Behinderung des Datenflusses – sei es nun im Bereich Malwarekontrolle oder Behinderung der Datenexfiltration – stellt fundamentale Prinzipien des Internets und des freien Datenverkehrs in Frage.

Die gezielten Cyberangriffe auf Estland und auf die Elektrizitätsversorgung und digitale Infrastrukturen der Ukraine Ende 2015 zeigen neue Cyberrisiken auf. Während der Angriff massiv und der Schaden beträchtlich war – in der Ukraine hatten eine Viertelmillion Menschen bis zu sechs Stunden lang keinen Strom – blieb eine klare Attribuierung unmöglich. Das Verdachtsmoment gegenüber russischen Akteuren stärkte lediglich die Bedrohungskulisse und erhöhte mit undiplomatischen Mitteln den politischen Druck auf die Ukraine. Viele Expertinnen und Experten bezeichneten den Angriff auf die Stromversorgung als Test, wie mit Cybermitteln kritische Infrastrukturen anderer Staaten angegriffen werden könnten mit dem Ziel, die Infrastruktur lahmzulegen und die Bevölkerung zu verunsichern.

Angesichts dieser Entwicklung und der zunehmenden Abhängigkeit der kritischen Infrastrukturen von digitalen Infrastrukturen muss der Staat seine Abwehrdispositive im präventiven und reaktiven Bereich überprüfen. Insbesondere geht es darum, das Risiko von Cyberangriffen mit flächendeckender Wirkung auf die Gesellschaft zu minimieren bzw. den Schaden im Eintretensfall durch resiliente Systeme zu reduzieren und die staatliche Handlungsfähigkeit zu sichern.

Die Zuweisung von Verantwortlichkeiten bei Cyberangriffen wird zunehmend dadurch erschwert, dass die Grenzen zwischen staatlichen, staatsnahen und privaten Akteuren verschwimmen, die im Auftrag handeln oder die vorhandenen Ressourcen und das Knowhow für eigene kriminelle Aktivitäten nutzen. Die digitalen Waffenarsenale der Geheim- und Armeedienste stellen insofern eine zunehmende Bedrohung dar, als sie durch Lecks der staatlichen Kontrolle entgleiten. Zivile nachrichtendienstliche und militärische Sphären vermischen sich. Die Nutzniesser sind kriminelle Akteure. Tatsächlich nahm die Cyberkriminalität in den vergangenen drei Jahren exponentiell zu.

Die fliessenden Grenzen ohne erkennbaren Gegner erschweren selbst bei einem präzisen Angriff auf die kritischen Infrastrukturen die Beurteilung, ab wann cyberbedingt von einer besonderen Lage ausgegangen werden muss. Es stellt sich die Frage, ab welcher Eskalation die zivilen Behörden bzw. die Armee originäre oder subsidiäre Hilfe leisten sollen. Der Aufbau von Kompetenzen und Ressourcen hat so zu erfolgen, dass die bisher bewährten Zuständigkeitsprinzipien nicht verändert werden müssen.

Die Enthüllungen von Edward Snowden und Wikileaks haben zur allgemeinen Erkenntnis und zum Bewusstsein geführt, dass Nachrichtendienste und andere staatliche Behörden die Digitalisierung und die neuen technischen Möglichkeiten dazu nützen, flächendeckend und auf Vorrat Daten zu sammeln. Die Bedrohung der massenhaften Ausspähung von in der Schweiz lebenden Personen und Staatsstellen stellt eine beträchtliche Souveränitätsverletzung dar. Dieses Risiko hat sich weiter akzentuiert, indem gewisse Länder ihre IKT-Industrie gesetzlich oder auf anderem Weg veranlassen können, vertraglich vereinbarte und/oder gesetzlich vorgeschriebene Geheimhaltungspflichten mit ihren Kunden nicht einzuhalten – und dies auch tun. Dies

führt dazu, dass im ohnehin schwierigen Umfeld der Cybersicherheit auch dem ehemaligen Sicherheits- und Geschäftspartner im IKT-Bereich kein 100-prozentiges Vertrauen mehr entgegengebracht werden kann. Die (Daten-)Supply-Chain wird zu einem Unsicherheitsfaktor.

Es muss davon ausgegangen werden, dass in einigen Ländern der Staat oder staatsnahe Akteure mit dem entsprechenden Wissen ihre Industrie im Technologiebereich dabei unterstützen, sich auf illegalem Weg geistiges Eigentum und geschäftskritische vertrauliche Daten von ausländischen Betrieben anzueignen; ebenso ist damit zu rechnen, dass sie ihre Unternehmen aktiv bei der Abwehr unterstützen und ungewollten Datenabflüssen nachgehen. Zwar haben die Nachrichtendienste und das Militär dieser Länder auch im analogen Zeitalter die heimische Industrie unterstützt. Im digitalen Zeitalter haben die Spionagemöglichkeiten im Cyberbereich aufgrund der Vorteile für den Angreifer (schwierige Attribuierung, mehrere Angriffsmöglichkeiten, Remote-Zugang) aber deutlich zugenommen. Dies kann auch im Fall der Industriespionage zu Wettbewerbsverzerrungen führen.

Nachdem der Europäische Gerichtshof das Safe-Harbor-Abkommen der Europäischen Kommission für ungültig erklärt hat, stellt das neue Privacy Shield-Abkommen einen Fortschritt dar. Die in die USA übermittelten Daten sind durch die durchgesetzten Prinzipien bei den teilnehmenden Firmen datenschutztechnisch besser geschützt. Die Schweiz konnte bei den USA ein vergleichbares Regime durchsetzen. Trotz grosser Kritik an der neuen Lösung – sie bringe gerade bei der kritischen Massenüberwachung keinen prinzipiellen Fortschritt – ist der Handlungsspielraum der Schweiz begrenzt, mehr Datenschutz einzufordern. Daher empfiehlt sich die Fortsetzung des bisherigen Ansatzes, sich an der EU zu orientieren. Damit kann zumindest eine gewisse Verhandlungsmacht gewahrt werden.

Der Staat hat verschiedene Möglichkeiten und Instrumente, den Schutz der Gesellschaft vor Cyberrisiken zu verbessern. Insbesondere sind zu nennen: die Definition und Umsetzung von Sicherheitsnormen und -standards, die Einführung von Meldepflichten, die Einrichtung einer zentralen Organisation, die bei Sicherheitsvorfällen unterstützt und informiert, die Unterstützung von Unternehmen und Forschungsstellen bei der Sicherheitsüberprüfung der Lieferkette bzw. einzelner Lieferanten im Bereich der digitalen Infrastrukturen und der Einsatz der Armee. Die Instrumente und Zielsetzungen sind an die jeweilige Zielgruppe – von den hochkritischen und kritischen Infrastrukturen über die relevanten Online-Dienste bis hin zu den Forschungsinstitutionen und der Privatwirtschaft – geeignet anzupassen. In den letzten eineinhalb Jahren sind die erwähnten Instrumente und Möglichkeiten Teil einer kontroversen Diskussion geworden.

8.2.2 Entwicklung im Ausland

Die zunehmende Bedrohung im Cyberraum und die Abhängigkeit kritischer Einrichtungen von digitalen Infrastrukturen haben viele Länder veranlasst, regulatorisch einzugreifen, Standards und Meldepflichten einzuführen und zentrale Organisationen aufzubauen. In Zusammenarbeit mit dem EDA hat die Expertengruppe einen Ländervergleich erstellt, der die Nachbarländer, die EU, die USA, China und ausgesuchte Länder in Skandinavien und in Asien berücksichtigt (s. Übersicht in Beilage 4).

Nicht überraschend haben autoritär geführte Länder in den letzten drei Jahren strikte Regulierungen durchgesetzt. So gelten dort für kritische Infrastrukturen und alle als relevant erkannten digitalen Infrastrukturen entsprechende Informationssicherheitsstandards und Meldepflichten. In den Vereinigten Staaten wurde mit dem sogenannten Cyber-Security Framework des National Institute of Standards and Technology (NIST)

ein relativ detaillierter Quasi-Standard für die kritischen Infrastrukturen eingeführt. Obwohl nicht explizit verpflichtend, üben die Sicherheitsvorschläge zusammen mit verschiedenen National Acts und State Laws einigen Druck aus und ermöglichen der Verwaltung regulierende Eingriffe bei privaten Betreibern.

Der massgebliche Standard für den europäischen Raum ist die Umsetzung der NIS-Richtlinie, die im August 2016 in Kraft getreten ist. NIS soll ein hohes Sicherheitsniveau von Netz- und Informationssystemen in der europäischen Union sicherstellen. Die Mitgliederstaaten müssen nationale Kontaktpunkte schaffen, Computersicherheits-Reaktionsteams-Stellen (CERTS) einrichten und Unternehmen identifizieren, die zur kritischen digitalen Infrastruktur gehören. Solche Unternehmen müssen angemessene technische Schutzmassnahmen (Sicherheitsstandards) vorsehen und Sicherheitsvorfälle melden. Diese Anforderungen gelten auch für Anbieter relevanter digitaler Dienste (Cloud-Betreiber, Suchplattformen, Online-Shop-Plattformen). Zurzeit fordern die Fachverbände in Deutschland eine Ausweitung der NIS-Regulierung im Rahmen des neuen IT-Sicherheitsgesetzes auf alle Unternehmen. Mit der Umsetzung von NIS wird auf breiter Ebene eine Kultur des IKT-Risikomanagements bei den Betreibern kritischer Infrastrukturen und relevanter Online-Dienste Einzug halten.

Bei allen Massnahmen spielt die Ausweitung des Adressatenkreises staatlicher Unterstützung und regulatorischer Auflagen eine entscheidende Rolle. Die NIS-Richtlinie hat mit der Berücksichtigung der Betreiber digitaler Dienste (Online-Shopping, Cloud, Suchplattformen) der digitalen Transformation Rechnung getragen und wichtige neue Akteure in die Pflicht genommen, die heute im Zuge der digitalen Transformation zur Versorgungssicherheit beitragen müssen. Dabei hatte NIS bisher hauptsächlich die grossen Anbieter Google, Amazon, Facebook und Apple (GAFA) im Blick. Diese Ausweitung führt auch zur Abgrenzungsschwierigkeit, wie weit der Definitionsspielraum für digitale Dienste gehen muss. Für Klein- und Kleinstunternehmen sind Ausnahmen vorgesehen. Trotz dieser de minimis Einschränkungen gehören Betriebe mit über 50 Arbeitnehmerinnen und Arbeitnehmern und einem Jahresumsatz von mindestens 50 Millionen Euro dazu. Grössere KMU mit einem Online-Portal für B2B Kunden stünden damit bereits in der Pflicht.

Viele Massnahmen der NIS-Regulierung haben bereits jetzt einiges zur Cybersicherheit beigetragen. Vor- und Nachteile insbesondere der Meldepflicht müssen aber noch genauer evaluiert werden. So ist in einigen Ländern die Anzahl der Meldungen merklich zurückgegangen. Die Unternehmen üben offenbar Zurückhaltung, weil sie weitere regulatorische Eingriffe und eine unnötige Verunsicherung des Markts befürchten.

8.2.3 Sicherheitsstandards, Normen und Massnahmen der guten Praxis

8.2.3.1 Im Bereich der kritischen Infrastrukturen

Die Nationale Strategie zum Schutz der kritischen Infrastrukturen und die Strategie zum Schutz der Schweiz vor Cyberrisiken haben den Schutz kritischer Infrastrukturen deutlich verbessert. Unter anderem liegen jetzt für alle kritischen Sektoren Verwundbarkeitsanalysen vor. Die Schweiz kennt aber keine allgemeinen cyberspezifischen Schutzbestimmungen im Sinne regulatorisch vorgeschriebener Standards für die kritischen Infrastrukturen. Entsprechend existiert auch keine zentrale Stelle, die sektorenübergreifend entsprechende Kompetenzen und Durchgriffsmöglichkeiten hat. Auch haben die meisten Sektoren keinen Regulator.

Auflagen und Pflichten sind, wenn überhaupt, sektoriell und spezifisch geregelt. So definieren zum Beispiel beim Flug- und Schienenverkehr interne Auflagen technische und organisatorische Massnahmen, da Schutz und Sicherheit oberste Priorität haben. Unter dem Eindruck der Cyberbedrohung hat auch die Finanzmarktaufsicht in ihren verpflichtenden Rundschreiben die Auflagen für mehr Cybersicherheit verschärft. Auch im Bereich der Telekommunikation sind die gesetzlichen Grundlagen vorhanden. Der Sektor Energie ist daran, über seinen Verband eine Lösung in Form eines Standards zu erarbeiten. In Zusammenarbeit mit der Wirtschaft wurde eine erste Bestandesaufnahme zum Standardisierungs- und Regulierungsbedarf in den verschiedenen Sektoren gemacht.

Nötig ist die Entwicklung verbindlicher und auditierbarer IKT-Sicherheitsstandards für alle Sektoren mit kritischen Infrastrukturen. Für die anderen Sektoren und die Betreiber relevanter Online-Dienste ist die Notwendigkeit verbindlicher und auditierbarer IKT-Sicherheitsstandards und deren Ambitionsniveau zu prüfen.

Im Detail müssen folgende Aspekte genauer betrachtet werden:

a) Energie, Verkehr, Finanzwesen, digitale Handelsplätze, Gesundheitswesen, Trinkwasserlieferung und -versorgung und wesentliche Dienste im Bereich Informationstechnik und Telekommunikation[13] müssen zwingend berücksichtigt werden.

b) In einem Sektor sind nicht alle Betreiber gleich kritisch. Deshalb ist eine Differenzierung zwischen den einzelnen Betreibern in Betracht zu ziehen und es sind entsprechende Kriterien zu erarbeiten.

c) Es ist zu prüfen, ob es unterschiedliche Standards für die einzelnen Sektoren braucht, da die Sicherheitsniveaus nicht überall gleich hoch sein müssen.

d) Der Frage ist nachzugehen, welche zentralen oder dezentralen Stellen die koordinierenden Aufgaben, aber auch die Durchsetzung von Standards sicherstellen können, wenn keine (Aufsichts-)Behörde vorhanden ist.

e) Es ist zu klären, inwiefern die Betreiber relevanter digitaler Dienste zu berücksichtigen und welche Regeln de minimis einzuführen sind.

f) Es ist zu prüfen, welche gesetzlichen Grundlagen nötig sind. Diese können sektorspezifisch sein oder wie in Deutschland oder Frankreich ein Rahmengesetz bilden.

Diese Entwicklung muss in Zusammenarbeit zwischen Behörden, Verbänden und der Privatwirtschaft erfolgen und auf bekannten Standardrahmenwerken und Ergebnissen aus Verwundbarkeitsanalysen aufbauen. Diese IKT-Standards sollten dort, wo es keine Aufsichtsbehörde gibt, durch die entsprechenden Fachverbände erarbeitet werden. Das Vorgehen zur Überprüfung der Einhaltung ist ebenso branchenweit zu regeln. Der Bund muss ein Kompetenzzentrum im Bereich der Cybersicherheit aufbauen, das diese Arbeiten begleiten und auch die Datenschutzaufsichtsbehörden beraten und unterstützen kann.

[13] In der NIS werden Internet Exchange Points (Internetknotenpunkte, IXP), Domain-Name-Dienstanbieter und Certificate Authorities berücksichtigt.

Empfehlungen:

25. Bund und Kantone erarbeiten in enger Zusammenarbeit mit den Fachverbänden auditierbare IKT-Sicherheitsstandards und verpflichten die Betreiber kritischer Infrastrukturen, diese Sicherheitsstandards zu beachten.

26. Der Bund baut ein Kompetenzzentrum (bzw. eine Stelle im Rahmen eines Kompetenzzentrums für Cybersicherheit) zu Fragen der Standardisierung im Bereich IKT-Sicherheit auf.

8.2.3.2 Im Bereich der breiten Wirtschaft

Die Maturität der digitalen Infrastrukturen muss in der Breite verbessert werden. Dies gilt im gleichen Umfang für Organisationen und Forschungsstellen wie auch für die private Wirtschaft und dort auch für mittlere und kleinere Unternehmen. Die Einführung von IKT- bzw. Informationssicherheitsstandards in Form eines IKT-Grundschutzes als „best Practices“ und Handlungsempfehlung würde zu einer deutlichen Verbesserung der Lage führen. Hierzu soll der Bund in enger Zusammenarbeit mit den Dach- und Branchenverbänden, mit den Verbänden der IKT-Anbieter und interessierten Unternehmen ein Programm zur Verbesserung der Informationssicherheit in der KMU-Welt lancieren.

Die Festlegung eines Standards durch den Staat hingegen widerspräche dem schweizerischen Grundverständnis von Wirtschaftsfreiheit. Zudem verlangt die Vielfalt der Branchen eine flexible Ausgestaltung möglicher Schutzmassnahmen in einem IKT-Grundschutz. Inwiefern eine Harmonisierung des Grundschutzes möglich ist, muss im Rahmen dieser Arbeiten mit allen Interessengruppen geklärt werden.

Empfehlung:

27. Der Bundesrat fördert in enger Zusammenarbeit mit den Dach- und Branchenverbänden, mit den Verbänden der IKT-Anbieter und mit interessierten Unternehmen Programme zur Verbesserung der Informationssicherheit in der Wirtschaft.

8.2.4 Meldepflichten

Ein integrales Lagebild und der Austausch aller Informationen über Cyberangriffe würden die Sensibilisierung entscheidend fördern und die Verwundbarkeiten reduzieren. Basis dafür wäre eine Meldepflicht von Cybervorfällen für alle Betreiber kritischer Infrastrukturen und relevanter digitaler Dienste. Die Schweiz kennt bisher keine allgemeine Meldepflicht. Erwähnt sei jedoch, dass Art. 22 E-DSG die Einführung einer Meldepflicht bei Verletzungen der Datensicherheit vorsieht. Einzig bei spezifischen Versorgungsunterbrüchen wie zum Beispiel im Fernmeldewesen sind Meldepflichten bekannt: Diese sind aber nicht auf die Erfassung von Cyberbedrohungen fokussiert.

Bei der Einführung einer Meldepflicht müssten im Detail folgende Fragen geklärt werden:

- Für wen gilt die Meldepflicht? Es braucht Kriterien für die Prüfung der Frage, ob alle Sektoren bzw. alle Betreiber in einem Sektor der Meldepflicht unterliegen.
- Ist eine allgemeine Meldepflicht in Betracht zu ziehen oder nur bei spezifischen Ereignissen (nicht zu verwechseln mit Schwere, s. nachfolgenden Punkt)? Die dafür notwendigen Kriterien sind zu definieren (z.B. Gefährdung der Öffentlichkeit oder Verlust von Daten, die der Non-Proliferation unterliegen).

- Ab welcher Schwere besteht eine Meldepflicht, und gilt diese Schwelle für alle Betreiber?
- Wem müssen die sicherheitsrelevanten Vorfälle gemeldet werden? Eine Meldepflicht sollte in erster Linie gegenüber den (Aufsichts-)Behörden und MELANI gelten. Da nur wenige Sektoren einen solchen Regulator kennen, müssen für die betroffenen Sektoren neue Stellen oder eine zentrale Stelle geschaffen werden.
- Fallen die Betreiber relevanter digitaler Dienste auch unter die Meldepflicht, und welche Kriterien gelten für sie?
- Welche gesetzlichen Grundlagen sind dafür zu schaffen? Diese können sektorspezifisch sein oder wie in Deutschland oder Frankreich ein Rahmengesetz darstellen.

Im Unterschied zur Meldepflicht drängt sich eine „Blame and Shame"-Einrichtung, wie z.B. der US Health Wall of Shame nicht auf. Eine allgemeine Information der Öffentlichkeit, auch soweit diese durch einen Vorfall gar nicht betroffen ist, im Sinne einer öffentlichen Anprangerung von „Sicherheitssündern", erscheint nicht erforderlich und entspricht auch nicht den schweizerischen Gepflogenheiten. Öffentliche Anprangerung könnte sich auch kontraproduktiv auswirken, indem sich Unternehmen veranlasst sehen könnten, Vorfälle nicht zu melden und zu vertuschen, um einer Blossstellung zu entgehen.

Empfehlung:

28. Der Bund führt für die Betreiber kritischer Infrastrukturen eine Meldepflicht für Cybervorfälle ein. Er erarbeitet dabei zusammen mit den zuständigen Behörden, der Privatwirtschaft und den Verbänden die Grundlagen und berücksichtigt die internationale Entwicklung.

8.2.5 Landesweite und zentrale Organisation zur Bewältigung von Cybervorfällen

Auf staatlicher Ebene funktioniert MELANI (Melde- und Analysestelle Informationssicherung) als Anlaufstelle und bietet Unterstützung bei der technischen und nachrichtendienstlichen Analyse der Vorfälle inklusive der dazugehörenden Informationsaustauschplattform.

Aufgrund der begrenzten Ressourcen gehören nicht alle Betreiber kritischer Infrastrukturen zum Kundenkreis von MELANI. Mit dem Ziel, den Kundenkreis zu erweitern, sollen die Relevanz der einzelnen Sektoren angesichts der digitalen Transformation geprüft und entsprechend die Ressourcen evaluiert und zugeordnet werden. Die Dienstleister der Sektoren Energie, Verkehr, Bankwesen, Betreiber von Handelsplätzen, Gesundheitswesen, Trinkwasserlieferung und -versorgung und digitale Infrastrukturen sind dabei zu priorisieren. In einer Erweiterungsrunde wären die Betreiber relevanter Online-Dienste zu evaluieren.

Die heute schon enge Zusammenarbeit mit den relevanten Kompetenzzentren (u.a. CERT) ist gezielt zu intensivieren, damit die beschränkten spezialisierten Ressourcen in der Schweiz möglichst effektiv und effizient genutzt werden können.

Aufgrund des Bedrohungsbildes muss die bisherige Zielgruppe kritische Infrastrukturen stark erweitert werden, u.a. auf Forschungseinrichtungen, die private Wirtschaft

und dort insbesondere auf die sensitiven Bereiche, wo Technologiespionage und Kundenschutz eine relevante Rolle spielen. Schliesslich muss auch die KMU-Welt miteinbezogen werden.

Die Dienste von MELANI, u.a. die Unterstützung bei Vorfällen, als Informationsstelle, als Beratungsstelle im präventiven Bereich und Informationsaustauschplattform, sind entsprechend auszuweiten und in einem eigentlichen Kompetenzzentrum des Bundes für Cybersicherheit zusammenzuführen. Die Umsetzung dieser bereits in der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022 formulierten Ziele muss schnell vorangetrieben werden.

Auch bei einem stark erweiterten Ausbau des Kundenkreises ist die bisherige Qualität beizubehalten und der vertrauensvolle Informationsaustausch mit den Betreibern kritischer Infrastrukturen zu gewährleisten. Es muss klar definiert werden, welche Kundenkreise aus welchen Sektoren Anspruch auf welche Dienstleistungen und Informationen haben. Denkbar wäre ein Zwiebelmodell, bei dem MELANI für die äusseren, weniger kritischen Kundenkreise vor allem Dienstleistungen im Bereich Prävention und Vorfallbewältigung entwickeln würde. Diese Unterstützung würde stets subsidiär zu den Angeboten im Bereich Schutz und Vorfallbewältigung, die auf dem Markt verfügbar sind, erfolgen. Mit dem Ausbau würde MELANI zu einem schweizweiten Cyber-Krisenmanagement-Organ, das entsprechend in die Struktur der Krisenstäbe des Bundes und der Kantone zu integrieren wäre.

Beim Aufbau eines landesweiten Zentrums sind folgende Fragen im Detail zu klären:

- Wie ist die Subsidiarität zu gewährleisten? Welche Stufen der Eskalation sind dafür zu unterscheiden? Entsprechende Dienste der Privatwirtschaft dürfen nicht unnötigerweise konkurrenziert werden.
- Orientiert sich die Definition der relevanten Eskalationsstufen nur an der Handlungsfähigkeit des Staates und dem Gemeinwohl der Gesellschaft oder auch an wirtschaftlichen Überlegungen?
- Welche Dienstleistungen sind welchen Kundenkreisen (breite Wirtschaft, KMU-Welt, Forschungsinstitute) bei welcher Lage zuzusprechen?

Empfehlung:

29. Der Bund sorgt in Zusammenarbeit mit den Kantonen, der Wirtschaft und den Forschungsinstituten dafür, dass mit dem Ausbau von MELANI ein landesweites Zentrum (bzw. eine Stelle im Rahmen eines Kompetenzzentrums für Cybersicherheit, s. Empfehlung 26) zur Prävention und Bewältigung von Cybervorfällen geschaffen wird.

8.2.6 Betriebssicherheitsverfahren für die Betreiber kritischer Infrastrukturen und weitere Anspruchsgruppen

Der Entwurf für ein Informationssicherheitsgesetz (ISG) sieht gemäss Botschaft die Durchführung von Betriebssicherheitsverfahren auch im nichtmilitärischen Bereich vor. Dieses Verfahren ermöglicht die Überprüfbarkeit der Vertrauenswürdigkeit von Betrieben, die Aufträge von Behörden entgegennehmen wollen. Damit würde zumindest die Sicherheitsüberprüfung von IKT-Lieferanten mit Sitz in der Schweiz verbessert, deren Hauptsitz aber im Ausland ist. Eine ganzheitliche Überprüfung der Lieferkette bleibt aber nach wie vor unrealistisch. Beim Betriebssicherheitsverfahren kommen ebenfalls Mittel der Nachrichtendienste zum Zug, um die sicherheitsmässige Eignung von Fir-

men zu prüfen. Bereits 2011 wurde das verpflichtende Verfahren für die Betreiber kritischer Infrastrukturen und deren Lieferanten angedacht, aber schliesslich verworfen. Angesichts der Snowden-Erkenntnisse und der Ereignisse in der Ukraine empfiehlt die Expertengruppe die Betriebssicherheitsverfahren breiter als Instrument der Sicherheit einzusetzen.

Empfehlung:

30. Der Bund prüft,

- ob Betreiber kritischer Infrastrukturen eine Betriebssicherheitserklärung vorweisen müssen;
- ob und wie das Betriebssicherheitsverfahren auch Stellen ausserhalb des Bundes und der Verwaltung bei sensitiven Beschaffungen zur Verfügung gestellt werden kann.

8.2.7 Grenzen staatlicher Abwehrmöglichkeiten

Der Mechanismus der Abschreckung, wie er auch aus dem atomaren Bereich bekannt ist, scheint sich auch im digitalen Bereich durchzusetzen. Die grossen Mächte bauen entsprechende Angriffs- und Verteidigungsarsenale auf. Da die Angriffe oft nicht zurückverfolgt werden können und eine diplomatische Eskalation aufgrund mangelnder Beweise wenig zielführend ist, sind geeignete Abwehrmassnahmen und das Wissen der Gegenseite, dass man selbst auch über entsprechende Mittel verfügt, relevant.

Der Handlungsspielraum der Schweiz ist eng: Zum einen ist die Schweizer IKT-Industrie, wie jene in den meisten Ländern, nicht in der Lage, eine umfassend sichere Zulieferkette (Supply-Chain) zur Verfügung zu stellen; zum anderen hat sie im Unterschied zu führenden Staaten in diesem Bereich keine entsprechenden Abwehr- oder Angriffsressourcen aufgebaut. Insofern sind die staatlichen Mittel begrenzt, um Einrichtungen der Forschung und der Wissenschaft sowie die sensitiven Bereiche der Wirtschaft – dazu gehören die kritischen Infrastrukturen, aber auch viele weitere für die Schweiz bedeutende Industriesektoren – bei der Cyberabwehr zu unterstützen. Europa und die Schweiz sind in Bezug auf die Hardware und zum Teil Software von den USA und von China abhängig.

Denkbar wäre der Aufbau eines Cyberzentrums, in dem mit dem entsprechenden Mitteleinsatz Angriffsvektoren und Gegenmassnahmen auf allen Ebenen untersucht und entwickelt würden. Dieses Zentrum könnte für die Betreiber kritischer Infrastrukturen entsprechende Lehrgänge anbieten. Allerdings gilt es zu bedenken, dass das Fehlen einer IKT-Sicherheitsindustrie in der Schweiz ein solches Projekt enorm erschweren und jede Inanspruchnahme von staatlichem oder privatwirtschaftlichem Knowhow aus dem Ausland die Unabhängigkeit wieder in Frage stellen würde.

Vor die Wahl gestellt, Geheimhaltungsauflagen einzuhalten bzw. Leistungserbringungen gegenüber Kunden im Ausland zu gewährleisten oder den Aufforderungen der eigenen Behörden (z.B. Nachrichtendiensten) zu folgen, Vertragsbruch zu begehen, dürften die meisten IKT-Leistungserbringer nicht lange zögern, letzterem Druck nachzugeben: Die Herausgabe von Daten der eigenen Kunden (Verletzung der Vertraulichkeit) oder die Einstellung/Verzögerung von Dienstleistungen (Einschränkung der Verfügbarkeit) sind die Folgen. Vor diesem Hintergrund kann man nicht mehr davon ausgehen, dass IKT-Leistungserbringer hundertprozentige Sicherheitspartner sind.

Um die Abhängigkeit vom Ausland bzw. ausländischen Firmen zu reduzieren, wäre der Aufbau von autarken digitalen Infrastrukturen in der Schweiz zu diskutieren. Denkbar wäre z.B. der Aufbau einer „Swiss-Cloud". Allerdings sind die Herausforderungen,

Kosten und Risiken bei einem solchen Projekt nicht zu übersehen: Je höher man den Anspruch bezüglich Unabhängigkeit vom Ausland ansetzt, desto weiter müsste der Anspruch gehen, von der Software über die Betriebssysteme bis hin zur Hardware bzw. dem einzelnen Chip die Komponenten zu überprüfen oder gar selbst zu entwickeln. Die Kosten wären enorm; denn nur schon ein paar Zeilen Programmiercode zu überprüfen kostet Zehntausende von Franken. Für die Überprüfung der Chips wäre der Aufwand um mehrere Grössenordnungen höher; u.a. wäre eine Infrastruktur nötig, die in der Schweiz im Moment nicht zur Verfügung steht. Zu betonen ist auch die Tatsache, dass die Eigenentwicklung von Software und Hardware „Kinderkrankeiten" mit sich bringen kann, die unter Umständen zu einem noch höheren Risiko führen als die genannte Abhängigkeit. Natürlich bieten sich Kompromisslösungen an, zum Beispiel der Ansatz, Opensource Software den eigenen Bedürfnissen anzupassen und aus Hardware-Komponenten verschiedenster Hersteller eine Cloud aufzubauen und in der Schweiz zu betreiben. Die Abhängigkeit von einzelnen ausländischen Herstellern würde allenfalls abnehmen, nicht aber die Bedrohung durch genau die Staaten, die Auslöser der Bemühungen waren. Diese könnten selbst auf Chip-Stufe „Backdoors" oder „Kill Switches" einbauen. In anderen Bereichen, etwa beim Aufbau eines Hochsicherheitsnetzes für die Schweiz, dürfte der Sicherheitsgewinn hingegen bei beträchtlich weniger Aufwand bedeutend sein (s. dazu auch Ziff. 4.4.3).

Die Botschaft zum neuen NDG unterstreicht, dass das Eindringen in Computersysteme und -netzwerke aussenpolitisch sensibel sein kann. Gelingt eine Attribuierung, könnte dies zu Retorsionsmassnahmen oder Gegenangriffen auf die Vertraulichkeit und Verfügbarkeit von digitalen Infrastrukturen und Daten in der Schweiz führen. Es ist deshalb festzuhalten, dass die Schweiz zurzeit über keine ausreichenden Mittel verfügt, um die digitale Souveränität zu garantieren. Für die Zukunft der Datenbearbeitung und der Informationssicherheit braucht es daher eine sicherheitspolitische Diskussion, wie dieser Herausforderung zu begegnen ist. Diese muss den äusserst ressourcenintensiven Aufbau eigener Abwehrmittel ebenso in Betracht ziehen wie die Möglichkeit, enge Kooperationen mit anderen Staaten einzugehen. Allerdings kann eine solche Kooperation ohne den Aufbau eigener Fähigkeiten zu einer Schutzschirmsituation durch diese Partner für die Schweiz mit den entsprechenden Abhängigkeiten führen.

Empfehlung:

31. Der Bund führt eine sicherheitspolitische Diskussion im Bereich Cybersicherheit darüber, ob und in welchem Umfang eigene Abwehrressourcen aufzubauen und/oder enge Kooperationen mit anderen Staaten einzugehen sind. Im Vordergrund soll dabei die Cyberresilienz stehen.

8.2.8 Aufgaben der Armee

Bei drohenden oder akuten Cyberattacken, welche zu ernsthaften Gefährdungen der Sicherheit in der Schweiz führen oder führen könnten, stellt sich die Frage, ob die Armee im Rahmen eines eigentlichen Verteidigungsfalls oder eines subsidiären Einsatzes (Assistenzdienst zur Unterstützung der zivilen Behörden) zum Einsatz kommen sollte.

Wenn Intensität und Ausdehnung einer Bedrohung in dem Umfang vorliegen, dass die territoriale Integrität, die gesamte Bevölkerung oder die Ausübung der Staatsgewalt gefährdet ist, kann von einem Verteidigungsfall gesprochen werden, auch wenn der Urheber der Bedrohung nicht unbedingt ein Staat ist. Im Rahmen einer Cyberattacke

durch Terroristen, Extremisten oder nicht klar zuweisbare Akteure aus der organisierten Kriminalität oder staatsnahen Bereichen kann ein Gegner seine Ziele auch durch die Beeinträchtigung der für das Funktionieren der staatlichen Institutionen, der wirtschaftlichen Abläufe und des gesellschaftlichen Lebens zentralen kritischen Infrastrukturen erreichen. Die Armee kann in einer solchen Situation einer ausserordentlichen Lage oder eines Notstandes originär zum Einsatz gelangen, wenn:

- die territoriale Integrität, die gesamte Bevölkerung oder die Ausübung der Staatsgewalt konkret bedroht oder gefährdet ist,
- es sich um eine zeitlich anhaltende Bedrohung handelt, die über eine bloss punktuelle zeitliche Bedrohung hinausgeht,
- es sich um eine landesweite, nicht bloss lokale oder regionale Bedrohung handelt, und
- die Bedrohung eine solche Intensität (Angriffsähnlichkeit) erreicht, dass sie nur mit militärischen Mitteln bekämpft werden kann.

Die Punkte sind kumulativ anzuwenden und können nicht als exakte Kriterien verstanden werden, die einen Automatismus bei der Entscheidung über einen originären Einsatz erlauben würden. Anhand dieser Anhaltspunkte hat der Bundesrat bzw. das Parlament situationsbezogen zu entscheiden.

Bei einer Cyberbedrohung, die diese Intensität und dieses Ausmass nicht erreicht, welche die zivilen Behörden in Zusammenarbeit mit der Privatwirtschaft jedoch nicht zu bewältigen in der Lage sind, kann die Armee auf Ersuchen der zuständigen zivilen Behörden namentlich bei der Sicherung und Unterstützung der kritischen Infrastrukturen Assistenzdienst leisten. Auch beim Assistenzdienst sind die Anhaltspunkte nicht als exakte Kriterien zu verstehen. Je nach Ausprägung entscheiden der Bundesrat, das VBS oder das Parlament über den Einsatz.

Auch angesichts neuer Cyberbedrohungen soll die Armee die strategische Reserve bleiben. Eine Verschiebung der in der Bundesverfassung festgelegten Kompetenz- und Aufgabenverteilung zwischen dem Bund und den Kantonen ist nicht vorzunehmen. Die zivilen Mittel beim Bund und den Kantonen sind aber so anzupassen, dass auch die neue Cyberbedrohung aufgefangen werden kann. Auch eine grössere Cyberbedrohung darf aufgrund fehlender Mittel nicht gleich als eine ausserordentliche Lage, eine Spitzenbelastung oder eine Katastrophe eingestuft werden. Entsprechende Kriterien sind zu überlegen, um – wie in der analogen Welt – ein Ambitionsniveau zu bestimmen, das im Bereich des Assistenzdienstes dem Gebot der Verhältnismässigkeit nach Art. 67 Abs. 2 des Militärgesetzes vom 3. Februar 1955 (MG) Sorge trägt und bei der Spontanhilfe nach Art. 52 Abs. 7 MG einen Einsatz ermöglicht.

Zudem sind die notwendigen Vorkehrungen zu treffen, damit im Bedrohungsfall ein optimales Zusammenwirken der verschiedenen staatlichen Kräfte (Armee, Polizei, Zivil- und Bevölkerungsschutz, Landesversorgung, etc.) gewährleistet werden kann.

Empfehlungen:

32. Der Bund trifft die nötigen Vorkehrungen, damit die Armee und die Militärverwaltung den zivilen Behörden subsidiär Mittel im Cyberbereich zur Verfügung stellen können. Diese sollen in ausserordentlichen Lagen die Betreiber kritischer Infrastrukturen unterstützen können.

33. Der Bund präzisiert die Kriterien für den verhältnismässigen Einsatz der Armee im Cyberbereich.

8.3 Schweizweite Harmonisierung des Datenschutzes für die Verwaltung

8.3.1 Kohärente datenschutztechnische Regelung für alle Verwaltungsstufen

Das DSG regelt die Bearbeitung von Personendaten sowohl durch private Personen als auch durch Bundesorgane (Art. 2 Abs. 1). Auf die Bearbeitung von Personendaten durch kantonale Organe ist das DSG – unter Vorbehalt von Art. 37 DSG – dagegen nicht anwendbar. Im Rahmen der Arbeiten zur Totalrevision des DSG wurde die Frage geprüft, ob diese Kompetenzverteilung zwischen Bund und Kantonen im Bereich des Datenschutzes noch adäquat ist oder ob eine Harmonisierung angestrebt werden soll, welche den Anwendungsbereich des DSG auf die kantonalen Organe ausweiten würde. Eine solche Erweiterung der Gesetzgebungskompetenz des Bundes im Bereich Datenschutz würde eine Teilrevision der Bundesverfassung voraussetzen. Auf Ersuchen der Vorsteherin des EJPD hat die Konferenz der Kantonsregierungen (KdK) zu dieser Frage eine Anhörung bei den Kantonen durchgeführt. Die Anhörung hat ergeben, dass eine Mehrheit der Kantone einer Ausdehnung des Geltungsbereichs des DSG auf Datenbearbeitungen durch kantonale Organe ablehnend gegenübersteht. Im Rahmen der Totalrevision des DSG wurde deshalb auf eine Anpassung der Kompetenzverteilung zwischen Bund und Kantonen (und auf die dafür nötige vorgängige Verfassungsrevision) verzichtet.

Die rasche Entwicklung bei der Datenbearbeitung macht aber deutlich, wie wichtig eine kohärente Regelung und die Möglichkeit einer raschen und flexiblen Anpassung und Durchsetzung des Datenschutzes sind. Das Risiko steigt, dass die Vielzahl kantonaler Regelungen dem entgegensteht. Vor diesem Hintergrund ist zu prüfen, ob und wie eine Harmonisierung zu erzielen wäre.

Empfehlung:

34. Der Bund prüft zusammen mit den Kantonen eine Harmonisierung des öffentlich-rechtlichen Datenschutzes in der Schweiz.

8.4 Staat als Dienstleister (E-Government)

8.4.1 Ist-Zustand, Risiken und Chancen

Seit über zehn Jahren verfolgen Bund, Kantone und Gemeinden eine aktive E-Government Strategie. Eine öffentlich-rechtliche Rahmenvereinbarung regelt die Organisation und das Vorgehen. Die jährlichen Statusberichte der Europäischen Kommission und

der UNO zum Stand von E-Governments zeigen einen kontinuierlichen Fortschritt. In den einzelnen Indizes befindet sich die Schweiz nicht in den Top 10. In der UNO Rangliste ist die Schweiz auf Platz 28 platziert und damit im hinteren Drittel im Vergleich mit den EU-Staaten.

Der differenziertere Länderstatusbericht der EU-Kommission bestätigt den Nachholbedarf. Bei den vier Hauptindikatoren Online Dienstleistungs- und Kundenorientierung (User Centricity), Leistungstransparenz (Benchmark Transparency), grenzüberschreitende Mobilität (Cross Border Mobility) und Basisinfrastrukturen (Key Enablers) befindet sich die Schweiz knapp unterhalb des EU-Durchschnitts. Im Bereich Leistungstransparenz und vor allem Basisinfrastrukturen wie elektronische Identität, elektronischer Dokumentenversand, Einmal-Erhebung von Daten mittels sicherer Zentralablage, sichere Ablagemöglichkeiten und Einmalanmeldung (Single Sign On) für verschiedene Seiten und Dienste sind die Beurteilungswerte der Schweiz bestenfalls mässig und z.T. ungenügend. Die verschiedenen Ratings stellen wertvolle Hinweise dar, welche Dienstleistungen in anderen Staaten aufgrund der Nachfrage wichtig und deshalb prioritär anzubieten sind. Hier ist die Schweiz gefordert, die Lücke zum europäischen Durchschnitt zu schliessen. Oberstes Ziel ist es, der Gesellschaft einen maximalen Nutzen durch die digitalen Dienstleistungen zu bieten, was auch der Wettbewerbsfähigkeit zugutekommt.

Die laufenden Projekte wie etwa die Schaffung eines Rechtsrahmens für ein staatlich anerkanntes E-ID-System, das Transaktionsportal für die Wirtschaft, eHealth Schweiz und eUmzugCH zeigen in die richtige Richtung, müssen aber beschleunigt, flächendeckend wirksam und zusammen mit den Basisinfrastrukturen konsequent weitergeführt und - entwickelt werden. Die überdurchschnittliche Dienstleistungsqualität der Behörden in der Schweiz und die ausreichenden Ressourcen für eine analoge bzw. hybride Abwicklung der Behördenleistungen haben bis heute zu keinem dringenden Handlungsbedarf mit Blick auf mehr E-Government geführt. Nichtsdestoweniger brächte eine forcierte Digitalisierung der Behördengänge der Verwaltung wie auch den juristischen und natürlichen Personen Prozesseffizienz, Zeit- und Produktivitätsgewinne, aber auch mehr Interaktion zwischen Bürgerinnen bzw. Bürgern und Staat. Wesentlich ist auch, dass E-Government auch für Menschen mit Behinderungen und Menschen mit altersbedingten Einschränkungen einen barrierefreien Zugang zu staatlichen Dienstleistungen – wie in der E-Government Strategie Schweiz definiert - gewährleistet. Hierbei bedürfen jedoch die sogenannten „Offliners“ einer besonderen Beachtung, damit diese nicht gesellschaftlich „digital“ benachteiligt bzw. ausgeschlossen werden.

E-Government darf sich sodann nicht darauf beschränken, den Dokumenten- und Informationsaustausch zwischen Staat und Entitäten sicher und digital zu gestalten. Es geht vielmehr darum, die Prozesse zwischen den Partnern ganzheitlich ohne Medienbrüche digital zu realisieren. Die Digitalisierung und die Anpassung der Prozesse würden die Automatisierung fördern, wo dies sinnvoll ist. Der digitalisierte Datenpool würde bedeutend anwachsen und zu Zweitverwendungen im Rahmen von Geschäftsmodellen oder verbesserten staatlichen Dienstleistungen führen. Intelligente Datenverarbeitung (KI, Big Data Analysen) könnte z.B. bei der Arbeitsvermittlung oder der effizienten Umsetzung der Sozialversicherungswerke die Behörden nachhaltig unterstützen.

Die Digitalisierung ist daher auch Anstoss, die analogen Prozesse zu überdenken und neu zu gestalten. Dies birgt Chancen für die Behörden, aber auch Risiken. Die Neugestaltung der Arbeitsweise und der dazu nötige Kulturwandel stellt für die betroffenen Stellen eine beträchtliche Herausforderung dar, was wiederum die Digitalisierung bremsen könnte.

8.4.2 Handlungsrahmen

Skaleneffekte der Digitalisierung sind nur zu erreichen, wenn die digitale Infrastruktur möglichst standardisiert ist und die Teilnehmerzahl eine kritische Grösse erreicht. Zentrale Entscheidungs- und Umsetzungsstrukturen bieten dafür ein günstiges Umfeld. So fällt bei den Vorreitern von E-Government – wie Dänemark, aber auch grösseren Ländern wie England – auf, dass der Erfolg auf einem Top-down System beruht, bei dem Ziele transparent und demokratisch festgelegt und übergreifend durchsetzt werden, wobei Bottom-up-Initiativen gefördert, koordiniert und in das grosse Ganze eingebettet werden. Erfolgreiches E-Government verlangt eine durchgängige Struktur mit einer partizipativen Koordination und Steuerung von den Gemeinden bis zum Bund. Das Zusammenführen von technischen Einzellösungen mit dem Anspruch der Interoperabilität ist in der Regel mit höheren Kosten, Verzögerungen und Umsetzungsproblemen verbunden. Ebenfalls wird die kritische Masse an Nutzern nicht erreicht. Das föderale System mit seinen fragmentierten Strukturen und dem Prinzip der Subsidiarität trägt wesentlich zum Erfolg der Schweiz bei. Es stellt einen systemischen Widerstand gegenüber zentralisierenden Tendenzen in der digitalen Transformation dar, aber es kann auch zu einer verbesserten Resilienz beitragen. Die technische und rechtliche Kompatibilität und Interoperabilität zu den Verhältnissen in der EU und der dortigen Digital-Entwicklung zum Single Market ist sicherzustellen.

Führung, Steuerung, Koordination
Die Organe, die sich momentan auf Bundesebene mit dem nationalen Thema E-Government beschäftigen, haben keine wirklichen Steuerungs- oder gar Durchsetzungsbefugnisse. Entsprechend findet eine wirksame Koordinierung der Aktivitäten im Bereich E-Government nicht statt. Dies muss verbessert werden, damit schnelle Fortschritte und digitale Skaleneffekte erzielt werden.

Basisinfrastruktur
Zur Basisinfrastruktur gehört eine E-ID mit qualifizierter Signatur, die den Schriftformerfordernissen genügt, ein Identity and Access Management, ein entsprechendes Single Sign On (Einmalanmeldestelle) bzw. ein Single Point (zentrale Anlaufstelle) für Private und die Geschäftsseite sowie eine sichere Daten- und Dokumentenablage, d.h. ein digitaler Briefkasten für alle Entitäten. Dieser digitale Briefkasten stellt einen bidirektionalen Online-Kommunikationskanal zwischen Behörden und allen Gesellschaftsteilnehmern sicher. Die Basisinfrastruktur muss flächendeckend verfügbar sein und Interoperabilität, Wirtschaftlichkeit, Sicherheit und Komfort sicherstellen, denn sie wird an der Benutzerfreundlichkeit der privatwirtschaftlichen Lösungen gemessen.

Die IKT-Systeme der Verwaltung sind in den letzten 30 Jahren organisch gewachsen. Sie spiegeln den föderalen Aufbau wider. Selbst in den einzelnen Kantonen bzw. in der Bundesverwaltung dürften die Infrastrukturen zu wenig leistungsfähig vernetzt und interoperabel sein, um den digitalen Anforderungen von E-Government und der Datenverarbeitung im 21. Jahrhundert zu genügen. Viele der heutigen Kernsysteme der digitalen Infrastrukturen wurden für analoge Prozesse ausgelegt und müssen von Grund auf erneuert werden. Das Ziel – mehr Effizienz, Synergien und Vernetzbarkeit – ist zu erreichen, indem die Verwaltungen Standards festlegen und bei übergreifender Nutzung gemeinsame Lösungen als Module erarbeiten. Dabei ist den Schnittstellen zu den Privaten Rechnung zu tragen.

Kritische Masse
Der Erfolg der digitalen Transformation in Estland, Dänemark, Finnland und Schweden zeigt sich daran, dass die erhofften Einsparungen bei einem gleichzeitig besseren, komfortableren und schnelleren Service bei Staat, Wirtschaft und Privaten allmählich erfolgreich realisiert werden. Grundlage und Voraussetzung dafür sind hohe Werte bei

der Erfassung aller Entitäten mit elektronischen Identifizierungsmitteln (E-ID), zentralen Anlaufstellen, Einmalanmeldestellen und einer ansprechenden Breite von Dienstleistungen, die alle relevanten und häufigen Behördengänge abdeckt.

Ein Vergleich der verschiedenen Umsetzungsstrategien in den E-Government-Vorreiterstaaten zeigt auf, welche Faktoren als erfolgsrelevant angesehen werden. Von den genannten Ländern verpflichten nur Dänemark und Estland ihre Einwohner, auf gesetzlicher Ebene eine E-ID zu haben. Ebenfalls haben nur diese beiden Länder ein de facto „Opt-out-System" bei den digitalen Behördenleistungen eingeführt. Das heisst, dass die Bürger bei einer Mehrheit von Behördengängen analoge Dienste nur noch auf Anfrage in Anspruch nehmen können. Als Folge werden 80-90 % der Behördengänge digital abgewickelt. Ähnlich hoch ist die Verbreitung der E-ID. Obwohl Finnland, Schweden und England diese rekordhohen Werte nicht erreichen, weisen sie auch ohne gesetzliche Auflagen eindrückliche Zahlen auf. Sie erreichen dies, indem sie ihre Einwohner standardmässig mit einer E-ID ausstatten oder die Anmeldung und den Erhalt schnell und komfortabel gestalten. Die E-ID ist überall gebührenfrei.

Ebenfalls fällt auf, dass die Organisation der E-ID-Vergabe in den verschiedenen Staaten entweder zentral oder dezentral organisiert ist. Beide Ansätze scheinen erfolgreich funktionieren zu können. In Schweden und England etwa stellen verschiedene private Dienstleister die E-ID aus. Ein entscheidender Erfolgsfaktor scheint hingegen zu sein, dass in allen genannten Ländern der Staat bei der E-ID nicht nur eine koordinierende und beaufsichtigende, sondern auch eine aktive Vorreiterrolle eingenommen hat. Er ist aktiv auf die privaten Anbieter zugegangen, hat eine technische Lösung vorangetrieben und gleichzeitig breite digitale Dienstleistungen angeboten, um eine kritische Masse von Nutzern zu erreichen. Alle genannten Staaten stellen für Private und die Geschäftsseite zentrale Anlaufstellen mit Einmalanmeldung zur Verfügung. Die Behörden relativieren den Mehraufwand für die Umstellung und die Vorbehalte digitalferner Bürgerinnen und Bürger dadurch, dass E-Government von der ersten Anwendung an dem Bürger weniger Komplexität und weniger Zeitaufwand verspricht und garantiert. In der Folge hat die private Wirtschaft die Lösung als Standard akzeptiert und dient nun selbst als Multiplikator.

Anschlussfähigkeit an den Digital Single Market der EU
Im Rahmen des Digital Single Market der EU spielt der Aktionsplan für E-Government eine wichtige Rolle. Grundlage und Treiber dafür sind die Entwicklung der Connecting Europe Facility (CEF) Building Blocks, die die digitalen Infrastrukturen eDelivery, E-ID, eInvoicing, eSignature und eTranslation beinhalten.

Empfehlungen:

35. Bund und Kantone schaffen für die digitale Transformation im Bereich der Behördentätigkeiten medienbruchfreie und einheitliche Rahmenbedingungen, die eine auch für Private und Wirtschaft möglichst benutzerfreundliche sowie gut koordinierte und vernetzte Datenbearbeitung unter Wahrung des Datenschutzes ermöglichen und, wo es sinnvoll erscheint, Lösungen schweizweit skalieren lassen

36. Bund und Kantone stellen sicher, dass bei der Umsetzung der E-Government-Strategie Schweiz die Bevölkerungsgruppe der „Offliner“ durch die Digitalisierung nicht gesellschaftlich ausgegrenzt wird.

8.5 Open Government Data und Open Data

8.5.1 Ist-Zustand, Risiken und Chancen

Open Government Data (OGD) verfolgen das Ziel, Daten der Verwaltung der Gesellschaft zur Wiederverwertung zur Verfügung zu stellen. Je offener, zugänglicher, auffindbarer und allgemein bearbeitbarer die Daten sind, desto mehr Nutzen erbringen sie: Dies kann zu neuen Geschäftsmodellen führen, ein Wirtschaftstreiber werden, die Forschung voranbringen und nicht zuletzt auch die Dienstleistungen der Behörden verbessern. Schliesslich trägt die Offenlegung der Daten auch dazu bei, die Arbeit der Behörden transparenter zu gestalten. Bei OGD sind Daten ausgenommen, die dem Datenschutz, dem Informationsschutz oder immaterialgüterrechtlichen Auflagen unterliegen. Schätzungen zufolge würden OGD als Wirtschaftstreiber dem BIP lediglich einen Zuwachs von 0,2 % bringen. Es ist aber davon auszugehen, dass OGD einen nicht zu unterschätzenden positiven Einfluss auf den Datenfluss hätten, etwa in den Bereichen Forschung und Informationsbeschaffung. Deren ökonomischer Wert muss jenseits quantitativer Berechnungen aus qualitativer Sicht als hoch bewertet werden.

Bereits 2014 hat der Bundesrat eine OGD-Strategie verabschiedet mit dem Ziel, bis 2018 u.a. die rechtlichen Rahmenbedingungen und die Gebührenpolitik zu überprüfen und entsprechende gesetzliche Grundlagen zu schaffen, eine koordinierte Publikation und die technischen Infrastrukturen bereitzustellen sowie den Weg für eine Open-Data-Kultur zu ebnen. Die Strategie soll auch Grundlage sein, um mit den Kantonen und Gemeinden eine Zusammenarbeit in Richtung umfassender OGD zu etablieren. Ein möglichst grosser und harmonisierter Datenpool über föderale Grenzen hinweg würde erst das ganze Potenzial von OGD freisetzen. Eine gesetzliche Querschnittsregelung kann der Bund an dieser Stelle nicht leisten, da er über keine entsprechenden Gesetzgebungskompetenzen verfügt.

Das aktuelle Rating der OECD zur Maturität der OGD verortet die Schweiz im hinteren Drittel. Die entsprechende Studie der EU (2015) bewertet die Schweiz als OGD Follower: Vision, Konzepte und technische Infrastrukturen liegen zwar vor, vieles ist aber noch ungelöst und die Datenmenge klein. Auch bedeutende private OGD Barometer wie der Open Data Barometer oder der Global Open Data Index reihen die Schweiz lediglich innerhalb der Top 50 ein, womit sich eine moderne Dienstleistungs- und Hochtechnologie-Gesellschaft wie die Schweiz nicht zufriedengeben darf. Die Ratings bemängeln einerseits die Datenqualität: Die Daten stehen überwiegend lizenztechnisch nicht frei zur Verfügung und Benutzer können die bestehenden Datensammlungen nicht auf einmal in einem offenen und maschinenlesbaren Format herunterladen.

Zudem stehen wesentliche Datensammlungen wie das Handelsregister, die Grundbücher oder die Geo- und Metadaten nicht vollumfänglich und frei wiederverwendbar zur Verfügung.

Auch bei der Zusammenarbeit mit den Kantonen gibt es Herausforderungen: Lediglich sieben Kantone haben bisher ihre Daten dem Single Point Portal zur Verfügung gestellt. Die Mehrzahl der Kantone hat noch keine Infrastrukturen, um ihre Daten aufzubereiten und auch nicht die rechtlichen Grundlagen. Nur eine Minderheit der Kantone hat bisher aktiv OGD vorangetrieben und intensiv mit dem Bund zusammengearbeitet. Fehlende Ressourcen und der Mangel an spezifischem Fachwissen sind als Gründe aufzuführen. Es ist aber auch davon auszugehen, dass sich eine Mehrzahl der Kantone in einer Wartestellung sieht und abwartet, bis eine Stelle die Führung übernimmt. Entsprechend viel Entwicklungspotenzial gibt es bei der Zusammenarbeit zwischen Bund und Kantonen.

Ein halbes Jahr vor Ablauf der OGD-Strategie (2014-2018) zeichnet sich ab, dass wichtige Ziele der Strategie nicht erreicht werden. Der bisherige Ansatz mit Spezialerlassen und Gesetzgebungsprojekten der zuständigen Behörden hat nicht zum Ziel geführt, in allen Bereichen innert Frist über rechtliche Grundlagen zu verfügen. Um die gesetzlichen Voraussetzungen für die Verwendung von mit öffentlichen Mitteln erhobenen Daten sicherzustellen, bieten sich verschiedene Alternativen an: Eine wäre die entsprechende Ausweitung des BGÖ, die andere die Schaffung eines nationalen Informationsverwaltungsgesetzes. Eine solche Normierung würde kohärente und sachgerechte Leitplanken setzen und die Rechtssicherheit dort fördern, wo die neuen Informationstechnologien generell das Verhältnis zwischen Staat und Bürgerinnen und Bürgern, Bund und Kantonen und auch Gemeinden im Kontext von Verwaltungs- und Verfassungsrecht herausfordern. Weitere Alternativen wären zu prüfen.

Gebührenfragen und damit auch Finanzierungsmodelle sind nach wie vor ungeklärt. Eng damit verbunden ist auch die Frage, inwieweit und unter welchen Bedingungen bundesnahe Betriebe zu OGD angeregt werden können, ohne das Prinzip verhältnismässiger Wettbewerbsbedingungen mit der Privatwirtschaft zu verletzen. Schliesslich müssen schweizweit alle verantwortlichen Stellen der Verwaltung die Koordination und den Austausch verbessern, um sich auf allgemeingültige definitorische und formattechnische Lösungen zu einigen.

Trotz Fortschritten behindern nach wie vor viele Barrieren das Potenzial der OGD. Prioritär zu nennen sind fehlende rechtliche Grundlagen, ungenügende Standardisierung bei der Datenaufbereitung, unklare Erfassung und unklare Nutzungsbestimmungen bei den Daten bundesnaher Betriebe sowie nicht ausreichende Ressourcen für die Umsetzung. Zusammenfassend muss die bisherige Zusammenarbeit von Bund und Kantonen als unzureichend eingestuft werden, um das nationale Projekt OGD voranzubringen.

Empfehlung:

37. Bund und Kantone schaffen die gesetzlichen Voraussetzungen, damit die mit öffentlichen Mitteln erhobenen Daten unter Wahrung der datenschutzrechtlichen Vorgaben für die weitere Verwendung erschlossen werden können.

38. Bund und Kantone richten eine Fachstelle ein, die Standardisierungen und Normierungen auf der technischen und operativen Ebene bei der Datenbearbeitung im Bereich OGD erarbeitet und alle betroffenen Verwaltungsstellen fachlich unterstützt.

8.6 Digitalisierte Demokratie

8.6.1 Ist-Zustand, weitere Entwicklung und Chancen

Die Auswirkungen der voranschreitenden digitalen Transformation durchdringen zusehends auch das historisch gewachsene Werte- und Normensystem unserer Demokratie.

Die rasante technologische Entwicklung und die daraus resultierenden neuen Möglichkeiten der gesellschaftlichen Interaktion von „Wissen“ und „Information“, verändern den breiten Kontext von Staat und Individuum im täglichen Zusammenleben. Die Beurteilung von E-Demokratie-Mechanismen steht erst am Anfang der Zeitgeschichte. In vielen Bereichen fehlt die Erfahrung, und das Abschätzen von Chancen, Risiken, daraus resultierenden Handlungsmassnahmen und Folgen lässt sich nur durch ein Vorgehen mittels „Versuch und Irrtum“ in der Praxis verifizieren. Eine Verordnung durch den Staat ist hierbei wenig zielführend. Daher ist über die Schaffung geeigneter Experimentierräume (z.B. in Form von Wettbewerben, Städteolympiaden etc.) nachzudenken, die im Rahmen eines subsidiären Systems gut realisiert werden könnten.

8.6.2 Herausforderungen und Risiken

Obwohl anfänglich von der Idee ausgegangen wurde, das Internet würde die Menschen befreien und zu einem besseren politischen Zusammenleben führen, dominieren heute manipulative Aspekte. Politiker, die „anders Denkende“ auf Twitter verunglimpfen; „Trolle“, die die Kommentarspalten der Medienportale mit Lügen füllen; Propagandisten, die verdeckt und raffiniert „alternative Fakten“ in den sozialen Medien verbreiten – die Möglichkeiten zur Manipulation von Individuen sind vielfältig.

Entsprechend ist im Zuge der digitalen Revolution die den öffentlichen Medien in einer Demokratie zugewiesene Aufgabe von besonderer Bedeutung: das Volk zu informieren sowie durch Kritik und Diskussion einen Beitrag zur Meinungsbildung und damit Partizipation zu ermöglichen. Allgemein besteht die Gefahr, dass die vierte Gewalt ihre für die Demokratie wichtigen Ziele zunehmend verfehlt: „Sie wird entweder weggeklickt oder sie setzt nur noch auf Sensation“. Die manipulativen Folgen sind „Fake News“, und der Wissensleser wird zum Informationskonsument, der sich mit nicht überprüften Informationen zufriedengibt. Zugänglichkeit, Verständniskomfort und Unterhaltungswert werden zunehmend prioritär. Auch lassen sich durch die Möglichkeiten des Profilings gezielt Gesellschaftsteilnehmer beeinflussen (Bubble Filter, Big Nudging, social Bots etc.) mit der Konsequenz, dass die kollektive Intelligenz unterminiert wird (s. auch Ziff. 11). Der Schritt von einer Informations- zu einer Wissensgesellschaft wird dadurch erschwert.

Ferner führt die Abhängigkeit von technischen Plattformen von „Monopolisten“, die zur Unterstützung von demokratischen Prozessen eingesetzt werden, zu weiteren schwer einzugrenzenden Beeinflussungsmöglichkeiten. Eigentlich stünden hier die „Big Player“, die Betreiber der Informationsplattformen, in der Verantwortung. Diese verstehen sich aber bestenfalls als neutrale Informationsvermittler. Für die Inhalte fühlen sie sich – in den meisten Fällen - nicht verantwortlich, obgleich es auch hier erste Ansätze im Sinne einer „Corporate Social Responsibility“ gibt.

Ergänzend oder als Alternative zu digitalen Plattformen, die von Unternehmen kontrolliert sind, würden sich öffentliche Plattformen anbieten. Solche Plattformen bieten eine Grundlage für kooperative Effekte sowie partizipative Demokratie (E-Partizipation). Die „City Challenge“ oder „City Olympics“ wäre ein nationaler, internationaler oder sogar globaler freundschaftlicher Wettbewerb, mit dem Gesellschaften innovative Lösungen zu wichtigen Herausforderungen zu finden versuchen. Wettbewerbsdisziplinen könnten beispielsweise die Reduktion des Klimawandels, die Entwicklung neuer, effizienter Energiesysteme, Nachhaltigkeit, Informationsvielfalt und deren Überprüfung, Resilienz oder Integration sein. Die im Wettbewerb über mehrere Monate mit öffentlicher Förderung erarbeiteten Lösungen sollten Open Source und Creative Commons sein, so dass sie von allen Städten, von Grossunternehmen, KMU und Spinoffs, Forschern, NGO und Zivilpersonen verwendet und weiter entwickelt werden können. Auf diese Art würde das Potenzial von Ansätzen wie Open Data, Open Access, Open Source, Open Science, Open Innovation, Hackathons, Fablabs, MakerSpaces, Gov Labs und Citizen Science auf ein völlig neues Niveau gehoben und damit auch die Möglichkeit zivilgesellschaftlicher Lösungsbeiträge geschaffen.

Insgesamt würde eine positive Aufbruchsstimmung erzeugt, die für eine erfolgreiche Transformation hin zu einer digitalen und nachhaltigen Gesellschaft erforderlich ist.

In naher Zukunft werden sich insbesondere folgende Fragen stellen: Wie und wo soll der Staat proaktiv die neuen digitalen Möglichkeiten - im Sinne einer „E-Demokratie 4.0“ – ausschöpfen bzw. fördern? Wie kann die Digitalisierung zu einer Erhöhung der Beteiligung am politischen Prozess beitragen? Wird die durch die digitale Mobilisierung ins Rollen gebrachte demokratische Teilnahme des Einzelnen wirklich verbessert und erleichtert? Besteht nicht vielmehr die Sorge, dass sich der bewährte „retardierende Faktor“ bei politischen Entscheidungsprozessen verändert und zu einer digitalen „Instantdemokratie“ führt? Könnten sich die Wählerinnen und Wähler (z.B. durch zu viele Abstimmungen) überfordert fühlen und sich womöglich danach sehnen, ihr „höchstpersönliches (Abstimmungs-) Recht“ an einen „digitalen Assistenten“ zu delegieren?

Im Rahmen der wissenschaftlichen Begleitforschung zu den langjährigen Pilotanwendungen des E-Voting konnten viele Erkenntnisse zu den Einflüssen des Abstimmens über Internet auf die Demokratieteilnehmenden und Abstimmungen gewonnen werden. Neben den Vorteilen einer flexibleren, ortsunabhängigen und in die verschiedenen Lebenssituationen eingebetteten Meinungsbildung sowie einer der brieflichen Abstimmung ähnlichen Abstimmungsteilnahme besteht möglicherweise die Gefahr, dass bestimmte Bevölkerungsgruppen mit der Entwicklung zur E-Demokratie „digital“ überfordert oder ausgegrenzt und dadurch entsprechend in ihren Grundrechten eingeschränkt werden. Im Zusammenhang mit E-Voting ist die Informationssicherheit eine der grössten Herausforderungen für eine flächendeckende Einführung. Weniger Erkenntnisse liegen hingegen zur Entwicklung im Gebiet der E-Initiative, E-Meinungsbildung, E-Unterlagen usw. vor, wobei gerade E-Collecting viel weitgehendere Auswirkungen auf die Demokratie haben könnte als die elektronische Mitbestimmung bei Wahl- und Abstimmungsprozessen.

Wahlen und das Recht der Bürgerin und des Bürgers auf politische Mitbestimmung gehören zu den höchsten Gütern in einer Demokratie. Es ist deshalb entscheidend, dass das Risiko von Wahlfälschungen möglichst klein und Abstimmungs- und Wahlresultate transparent und nachvollziehbar sind. Die Akzeptanz von Wahlergebnissen ist eine Grundvoraussetzung für eine funktionierende Demokratie. Angesichts zunehmender Cybervorfälle nimmt in der Gesellschaft die Sorge um die Sicherheit demokratischer Prozesse zu.[14]

Die gemäss Verordnung der Bundeskanzlei vom 13. Dezember 2013 über die elektronische Stimmabgabe (VEleS) verlangten Schutzbestimmungen bei E-Voting Systemen basieren auf Vertrauensannahmen und der Unabhängigkeit von vier Kontrollkomponenten:

- die Anwendung unterschiedlicher Hard- und Software sowie unterschiedlicher Betriebssysteme,
- die Segregation der Netzwerke für die einzelnen Komponenten,
- die Anwendung möglichst einfacher Software, die auf die kryptographischen Funktionen eingeschränkt ist, und
- die strikte Trennung des Betriebs von der Systemüberwachung mit den entsprechenden organisatorischen Massnahmen beim verantwortlichen Personal.

Will ein Angreifer die Wahl unbemerkt manipulieren, muss er alle vier Kontrollkomponenten korrumpieren. Das Kontrollsystem der universellen Verifizierung lässt allfällige Manipulationen aufgrund von Inkonsistenzen erkennen.

Eine solche Manipulation aller vier Kontrollkomponenten setzt einen mächtigen Akteur voraus, der über ein umfassendes Knowhow verfügt und bereit ist, bedeutende Ressourcen zu investieren. Aus Sicht eines informationstheoretischen Sicherheitsanspruchs (s. auch Ziff. 4.2.1.6) kann man einen solchen Fall nicht ausschliessen, allerdings muss die spezielle Qualität dieser tendenziell eher theoretischen Bedrohung bei einer Bewertung des Risikos auf der operationellen Ebene berücksichtigt werden.

Auch wenn keine Inkonsistenzen feststellbar sind, können Interessenparteien mit Verweis auf dieses Risiko die Richtigkeit des digitalen Abstimmungsergebnisses generell anzweifeln und eine Abstimmungswiederholung verlangen, allerdings dürfte dieser Anspruch auf weniger Zustimmung in Gesellschaft und Politik stossen als im zweiten Szenario.

Dieses geht davon aus, dass das Detektionssystem Unregelmässigkeiten gefunden hat. Dieses Risiko hat im Unterschied zum ersten Szenario die Qualität eines wahrscheinlichen schlimmstmöglichen Falles. Ursache dafür können die Kompromittierung des Systems, aber auch technische Fehler oder menschliche Fehlmanipulationen sein, die zu Inkonsistenzen innerhalb der vier Kontrollkomponenten geführt haben. Bewegen sich die inkonsistenten Abstimmungsresultate ausserhalb einer gewissen Toleranz, könnte der Ruf laut werden und in der Bevölkerung auf Zustimmung stossen, dass die Abstimmung wiederholt werden müsse. Eine Häufung solcher Abstimmungswiederholungen würde das demokratische System beträchtlich belasten und letztlich das ganze E-Voting in Frage stellen. Auch ohne Hinweise auf vorsätzliche Kompromittierung kann jede Unregelmässigkeit zu einer Grundsatzdiskussion führen, politische

[14] u.a. in der Studie der ETH und der Schweizer Armee: Sicherheit 2018: Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend. Tibor Szvircsev Tresch und Andreas Wenger (Hg.). Zürich 2018.

Ängste vor Manipulation schüren und die Kritik an der Verlässlichkeit digitaler Systeme anwachsen lassen.

Die breite Einführung von E-Voting setzt voraus, dass die Gesellschaft hinreichend über die technischen und politischen Risiken informiert ist. Gleichzeitig muss die technische Ausgereiftheit bezüglich Stabilität und Verfügbarkeit so hoch sein, dass das Restrisiko im Rahmen der gesellschaftlichen Akzeptanz bleibt.

8.6.3 Erkenntnisse

Neue „innovative“ Ansätze zur Basisdemokratie, wie ein zeitgemässes Upgrade durch eine sogenannte „Massive Open Online Deliberation“ (MOOD) könnten in den Vordergrund des staatlichen Handelns treten. Dies würde der Demokratie erlauben, alle Argumente auf einen virtuellen Tisch zu bringen und verschiedene Perspektiven herauszukristallisieren sowie innovative, integrierte Lösungen zu erarbeiten. Die verschiedenen Gemeinwesen könnten dann die jeweils passendste Lösung wählen. Der gesamte Prozess kann auch von künstlichen Intelligenzsystemen unterstützt werden. Im Ergebnis entstehen Lösungen, die besser als Top-down- oder Mehrheitsentscheidungen sind, da sie auch berechtigte Einwände und Ideen von Minderheiten berücksichtigen. Während das konsensuale politische System der Schweiz einen solchen Ansatz im Wesentlichen bereits verfolgt, verspricht der Einsatz digitaler Technologien eine erhebliche Beschleunigung der entsprechenden Entscheidungsfindungsprozesse bei weiter verbesserten Partizipationsmöglichkeiten.

Empfehlungen:

39. Bund, Kantone und Gemeinden treffen geeignete Massnahmen, um Pilotprojekte mit innovativen Ansätzen der partizipativen Demokratie wie „Massive Open Online Deliberation“ zu fördern und Grundlagen für deren Beurteilung zu schaffen.

40. Bund, Kantone und Gemeinden fördern offene und partizipative Systeme und Prozesse (z.B. Open Data, Open Access, Open Science, Open Innovation, Citizen Science, Hackathons, Fablabs, Makerspaces, Gov Labs und City Challenges), um gesellschaftliche Ziele wie digitale Transformation, Resilienz und Nachhaltigkeit schneller zu erreichen.

41. Bund und Kantone dehnen E-Voting-Projekte nur aus, wenn aufgezeigt werden kann, dass E-Voting nicht mit grösseren Risiken verbunden ist als die bestehenden Formen der demokratischen Mitwirkung bei Wahlen und Abstimmungen. Wahl- und Abstimmungsergebnisse müssen überprüfbar bleiben.

9 Analysefeld Blockchain

9.1 Technologie und Infrastruktur

9.1.1 Ausgestaltung von Blockchain

Blockchain ist wörtlich verstanden eine Kette von Datenblöcken, die gemeinsam eine organisierte Datenstruktur bilden, die dezentral verwaltet wird, um Transaktionen sicher, verifizierbar und ohne zentrale Steuerstelle unabhängig durchzuführen. Jede Transaktion ist zwecks Unverfälschbarkeit und globaler Verifizierbarkeit elektronisch zu signieren. Neue Transaktionen werden jeweils am Ende der gegebenen Datenstruktur blockweise und chronologisch angehängt. Ein neu angefügter Block nimmt durch einen kryptografischen Fingerabdruck auf den vorherigen Block Bezug, womit eine nachvollziehbare und eindeutige Kette von Blöcken entsteht.

In neuerer Zeit wird oft von „Ledger“ (Register) gesprochen, weil Blockchain wie ein Registerbuch funktioniert (Aufzeichnung und Speicherung der Transaktionen). Die Abwicklung kann in einem Peer-to-Peer-Netzwerk ohne Intermediäre erfolgen. Sachlich zutreffender wäre deshalb der Begriff der „distributed Ledger Technology“, doch ist weiterhin der ältere Begriff Blockchain gebräuchlich.

Die an der Blockchain-Technologie Beteiligten müssen sich darauf einigen, wie die Reihenfolge der Blöcke auszugestalten ist, und sicherstellen, dass sich einmal ausgeführte Blöcke nicht mehr aus der Blockchain entfernen lassen. Die Teilnehmer erbringen grundsätzlich mittels eigener Rechenleistung einen „Proof of Work“, der gegen Fälschung schützt.

Andere Ausgestaltungen der Blockchain-Technologie sind verfügbar, doch haben sie sich in der Praxis noch kaum durchgesetzt: Dazu zählen insbesondere der „Proof of Space“ (Abstützung auf Speicherplatz statt Rechenleistung) und der „Proof of Stake“ (Relevanz des Stimmgewichts der Teilnehmer gestützt auf die Anzahl Transaktionen). Hingegen sind technische Anpassungen in der Praxis bedingt möglich, wie die am 1. August 2017 erfolgte Abspaltung von Bitcoin Cash (sog. „Fork“), die ein neues Protokoll und damit grössere Datenblöcke zur Bewältigung steigender Umsatzvolumen ohne Zeiteinbussen zulässt, gezeigt hat.

9.1.2 Technologische Herausforderungen

Von der Funktion her betrachtet stellt die Blockchain-Technologie eine (neue) Infrastruktur dar. Deshalb ist zu gewährleisten, dass grundsätzlich alle Interessierten Zugang erhalten und dass die (eventuell verschlüsselt) gespeicherten Daten den Berechtigten, aber auch nur ihnen, zugänglich sind. Weil Blockchain auf Intermediäre (Drittparteien, die als „Verwalter“ fungieren) grundsätzlich verzichtet, muss die Abwicklung von Transaktionen mit digitalen Inhalten sicher und effizient ausgestaltet sein. Im Gegensatz zur verbreiteten „open Blockchain", die überhaupt keinen Dritteinfluss kennt, sind bei der „permissioned Blockchain", die künftig an Bedeutung gewinnen könnte, einzelne Funktionen für Intermediäre vorgesehen.

Die Abwicklung der Transaktionen erfolgt unter Anwendung von kryptografischen Verfahren. Im Vordergrund steht die asymmetrische Verschlüsselung und Signatur (s. Ziff. 4.4.1), die von den Beteiligten einzusetzen ist. Die verkehrsüblichen Sicherheitsstandards sind bei Blockchain-Vorgängen zur Anwendung zu bringen.

In Weiterentwicklung der von virtuellen Währungen (z.B. Bitcoin) verwendeten Blockchain ist heute auch die Schaffung von sog. „colored Coins“ möglich; dabei wird einer minimalen Übertragung von Bitcoins zusätzlich über ein Eingabefeld ein „Token“ (z.B. eine Aktie) „angehängt“; der Transfer der Bitcoins dient hernach als Beweis der Übertragung des Eigentums an der „angehängten“ Aktie.

Andere Systeme (z.B. Ethereum) ermöglichen die Definition von beliebigen „Tokens“, die unabhängig voneinander sind und auch nicht an andere Werte „angehängt“ werden müssen. Dadurch lassen sich vorteilhaft Programme und Bedingungen beliebig umschreiben, etwa im Kontext von mittels Smart Contracts abgewickelten Transaktionen. Bei Smart Contracts beinhaltet die Blockchain zusätzlich noch Algorithmen, welche Übertragungsregeln oder Transaktionen definieren können, die automatisch ausgeführt werden, falls gewisse Bedingungen erfüllt sind.

9.1.3 Dezentrale Infrastruktur ohne staatliche Kontrolle

Die „distributed Ledger Technology" ist bewusst als dezentrale Infrastruktur ausgestaltet, d.h. es fehlt eine Organisation, die zentral Vertrauen zu schaffen vermag. Insbesondere kann der Staat keine Kontrolle über die abgewickelten Vorgänge ausüben, weil ihm mit Blick auf das dezentrale globale Netz die technologischen Möglichkeiten dazu fehlen.

Der Einsatz von Blockchain setzt also das Vertrauen der Bevölkerung in die Funktionsfähigkeit des technischen Systems voraus, ohne dass der Staat einen Beitrag zur Stärkung des Vertrauens leisten könnte. Insoweit geht es mithin auch um eine gesellschaftspolitische Werteentscheidung.

9.1.4 Sicherheitsaspekte der Blockchain-Technologie

Da Blockchain auf asymmetrischen kryptografischen Mechanismen beruht, stellt die Postquantumkryptografie auch für sie eine Herausforderung dar (s. Ziff. 4.4.1). So lässt sich nicht davon ausgehen, dass die Blockchain-Technologie langfristig Sicherheit bietet. Das Risiko verschärft sich dadurch, dass die Blockchain-Mechanismen keine Aktualisierungsmöglichkeit vorsehen. Die Grundstruktur von Blockchain ist anonym und nicht definiert. Zumindest bei der open Blockchain gibt es keine übergeordneten Instanzen, die bei einer einschneidenden Entwicklung der Kryptografie das System aktualisieren können. Dies wäre nur durch die Implementierung eines neuen Verschlüsselungssystems und einer Umverschlüsselung der ganzen Blockchain zu realisieren. Vor diesem Hintergrund müsste bei jedem Blockchain-Projekt ein Aktualisierungsmechanismus implementiert werden; denn lässt sich der Verschlüsselungsmechanismus nicht erneuern, ist die Nachvollziehbarkeit von Wertetransaktionen nicht mehr sicher.

Allerdings steht diese Notwendigkeit im Widerspruch zu einem der Sicherheitsprinzipien und zu den Vorteilen der open Blockchain: Keine zentrale Instanz soll die Möglichkeit haben, die Blockchain zu verändern. Nötig wäre deshalb ein Mechanismus, um Blockketten umschreiben und gleichzeitig böswillige Änderungen verhindern zu können, was eine Zusammenarbeit aller dezentralen Verifizierungsstellen (Schürfer) und der Kerngemeinschaft voraussetzt. Bei der „permissioned bzw. private Blockchain" mit einem zentralen Administrator der Schlüsselverwaltung stellen sich diese Herausforderungen nicht, indes profitiert diese Infrastruktur auch nicht von der dezentral angelegten Sicherheitsarchitektur der open Blockchain. Bei dieser Anwendung ist die Blockchain vom Sicherheitslevel der umliegenden digitalen Infrastrukturen abhängig und bringt nicht per se einen Sicherheitsgewinn.

Neben der asymmetrischen Verschlüsselung ist auch der Sicherheitslevel der Prüfsummen (Hashwerte) an die Fortschritte in der Kryptografie anzupassen. Mit dem Schritt vom aktuellen SHA-256 Standard zu SHA-384 wäre die Sicherheit auch bei einer ersten Generation von Quantencomputern gegeben.

Angriffe auf die Gesamtintegrität einer Blockchain sind möglich, indem ein Angreifer bei der Verifizierung und Validierung eines neuen Blockes beim „Schürfen" („Mining") die Kontrolle über 51 % aller Schürfer erreicht und stets seine Blöcke anhängen und durchsetzen kann. Allerdings setzt dieses Angriffsszenario bei den grossen Kryptowährungen enorme Rechenkapazitäten über eine längere Zeitspanne voraus, was die Profitabilität der Angriffe relativiert.

Öffentlich zugängliche Blockchains, vor allem Initial Coin Offerings und Kryptowährungen, stellen aufgrund der Angriffsfläche und der dort eingestellten Werte ein lohnenswertes Ziel dar. So werden Tauschbörsen für Kryptowährungen immer wieder erfolgreich angegriffen. Es fehlen klare Sicherheitsstandards, die das System und alle Anleger schützen. Allerdings zeigen die Regulierungsversuche Chinas, wie schwierig es ist, die digitalen Tauschbörsen zu kontrollieren und zu regulieren: Kaum waren sie in China verboten, wurden die Tauschbörsen unter anderem Namen in Hongkong wiedereröffnet. Sicherheitsprobleme gibt es auch bei der Sicherheit der digitalen Brieftaschen („Wallet") der Kryptowährungsinhaber, die immer wieder angegriffen werden. Entsprechende Sicherheitswarnungen für den Kunden wären ein möglicher Ansatz, um dieses Risiko zu reduzieren.

Gemeinhin wird Blockchain als zukunftsträchtige Technologie für Registeraufgaben gesehen, wie etwa für das Grundbuch, das Handelsregister oder allgemeiner für die Besitzhistorie von wertvollen Gütern (s. Ziff. 9.3.3). Angesichts der ungelösten Sicherheitsfragen ist die Praxistauglichkeit der Blockchain für solche Aufgaben mit einem mitunter sehr weiten Zeithorizont zumindest in Frage zu stellen. Der Verlust des kryptografischen Schlüssels führt im schlimmsten Fall dazu, dass die Besitzverhältnisse nicht mehr klar nachvollziehbar sind. Dies kann zur Unverkäuflichkeit des Gegenstands oder zu einer unrechtmässigen Werteübertragung führen. Es wäre bei allen Vorteilen der Blockchain-Technologie problematisch, relevante Infrastrukturen der Rechtssicherheit vorbehaltlos einer solch sicherheitsanfälligen Technologie anzuvertrauen.

Bei der Anwendung der Blockchain-Technologie ist zu berücksichtigen, dass sie in ihrer Grundstruktur die Sicherheitsattribute Integrität und Nachvollziehbarkeit abdeckt. Dies stellt gegenüber Datenbanken einen Vorteil dar, da die Rückverfolgbarkeit der Transfers in der Blockchain anders als in der Datenbank ein inhärentes Systemelement ist. Auch ist die Blockchain bei der Notwendigkeit dezentraler Systeme und allenfalls fehlerhafter Rechner das fehlertolerantere System als eine herkömmliche Datenbank. Doch auch die Nachteile sind nicht zu übersehen. Die Daten in der Blockchain selbst sind für alle zugänglich und sichtbar, womit Vertraulichkeit nicht gegeben ist. Für Anwendungen mit Auflagen an die Vertraulichkeit (Wahlen, Anwendungen im Bereich des Registerharmonisierungsgesetzes vom 23. Juni 2006 [RHG] oder des Datenschutzes, s. auch Ziff. 9.4.1) müssen ein entsprechendes Identitäts- und Zugangsmanagement sowie ein Verschlüsselungssystem implementiert oder separat eingesetzt werden. Beides kann die Sicherheit gefährden, was den Mehrwert der Blockchain aus Sicht des Sicherheitsaspekts wenn nicht in Frage, so doch zumindest zur Diskussion stellt.

Die Vorteile der Blockchain bei der Verwaltung von Transaktionen liegen in der klaren Spezifikation, welche Transaktionen ausgeführt wurden. Smart Contracts sind eine Er-

weiterung, welche die Regeln der Transaktion durch einen Algorithmus definiert. Sobald die Konditionen der Transaktion erfüllt sind, wird die Transaktion automatisch ausgeführt. Ein Risiko solcher Smart Contracts besteht in einer ungenügenden Abhandlung aller möglichen Situationen. Soll die Blockchain Infrastruktur künftig komplexe und sensitive Aufgaben gerade im Vertragswesen übernehmen, dann müssen die Sicherheit verbessert und entsprechende Systeme zur Qualitätssicherung entwickelt und verbindlich implementiert werden.

Empfehlung:

42. Bund und Kantone stellen sicher, dass Blockchain-Lösungen bei sensitiven Anwendungen in der Verwaltung und in regulierten Bereichen nur dann zur Anwendung kommen, wenn eine langfristige Sicherheit (z.B. rechtzeitige Aktualisierungen) gewährleistet ist.

9.2 Bisherige Regulierungsbemühungen

Die Blockchain-Technologie stellt eine globale Infrastruktur zur Verfügung. Aus diesem Grunde wären globale Regulierungen effizient. Realpolitisch ist aber eine entsprechende multilaterale Vereinbarung nicht zu erwarten.

Folgende (zwischen)staatliche Aktivitäten sind bemerkenswert: Vielfältige Initiativen gehen auf internationale Finanzorganisationen zurück, die von den virtuellen Währungen betroffen sind, etwa den Internationalen Währungsfonds und das Financial Stability Board. Das Europäische Parlament hat im Mai 2016 einen detaillierten Bericht zu den virtuellen Währungen veröffentlicht. Besonders aktiv sind die Organisationen in Grossbritannien: Ein fast 100-seitiger Bericht der Regierung vom Januar 2016 diskutiert Chancen und Risiken der distributed Ledger Technology; auch die Bank of England und die englische Financial Conduct Authority beschäftigen sich intensiv mit der Thematik.

Im Vordergrund der regulatorischen Bemühungen stehen aber die Tätigkeiten von privaten Organisationen, insbesondere die Selbstregulierungen durch Standardisierungsorganisationen. Abgesehen von einem Projekt der Linux Foundation ist vor allem die International Organisation for Standardisation (ISO), gestützt auf einen detaillierten Antrag von Standards Australia (einer nichtstaatlichen Organisation), durch das ISO Blockchain Committee aktiv, das sich darum bemüht, internationale Standards für die Blockchain-Technologie auszuarbeiten.

Gesamthaft betrachtet sind aber die Rechtsunsicherheiten in der Blockchain-Technologie weiterhin relativ gross, wie nicht zuletzt der Eingriff von Ethereum in die Technologie im Nachgang zu deren missbräuchlicher Ausnutzung durch eine Dezentrale Autonome Organisation (DAO) im Sommer 2016 gezeigt hat.

9.3 Von der Blockchain-Technologie besonders betroffene Rechtsbereiche

9.3.1 Virtuelle Währungen

Die grösste praktische Bedeutung hat die Blockchain-Technologie bisher im Kontext der virtuellen Währungen (v.a. Bitcoin) erlangt. Die Bitcoin-Blockchain ist als eine offene Datenbank ausgestaltet; weder wird der Zugang kontrolliert, noch bedarf es einer

namentlichen Registrierung mit dem eigenen Namen. Jeder Zahlungsvorgang wird auf der Blockchain als buchhalterischem Registerbuch vermerkt.

Die Sicherheit der Transaktionsabwicklungen wird durch eine Computer-Validierung, basierend auf einer mathematischen Aufgabe, gewährleistet; der ausgestellte Bitcoin lässt sich dann nur an einen einzigen Adressaten übermitteln. Dieser Vorgang ist rechenaufwendig und damit nicht sehr effizient und ist zudem teuer und langsam, weshalb zu erwarten ist, dass die Entwicklung neuer Algorithmen künftig zu besseren Verfahren führt.

Je nach Geschäftsumfeld ist eine vollständige Anonymität wie bei der traditionellen Verwendung von Bitcoin unerwünscht, weil sich die Geschäftspartner kennen wollen und auch die Behörden (z.B. Zoll, Steuerbehörden) interessiert sind, über die Identität der handelnden Personen/Unternehmen informiert zu sein. Deshalb sind z.B. IBM und Microsoft daran, Blockchains mit Zugangskontrolle zu entwickeln, die nicht zuletzt für die Handelsfinanzierungen der Banken (Trade Finance) von Bedeutung sein können. Zugang zu Blockchain erhält nur, wer über eine spezifische Berechtigung verfügt. Meist geht es bei solchen Infrastrukturen nicht um reine „Bezahlsysteme“, sondern die ganze Warenlieferungsabwicklung erfolgt über Blockchain.

9.3.2 Verhältnis Staat – Individuen

Diskutiert, aber noch nicht praktiziert wird die Verwendung der Blockchain-Technologie für die Durchführung von Wahlen. Die Zurückhaltung in der realen Welt ist der Notwendigkeit, einen hohen Grad an Datenintegrität zu gewährleisten (Einhaltung von Sicherheitsstandards), geschuldet. Im Vergleich zu anderen Ländern haben die Erfahrungen in der Schweiz gezeigt, dass der Versuch, elektronische Wahlmöglichkeiten einzuräumen (E-Voting), nicht leicht mit der Einhaltung des Legalitätsprinzips und der Wahrung der Abstimmungsfreiheit zu vereinbaren ist. Informationssicherheitsstandards müssen das Stimmgeheimnis schützen und technische Risiken der Ergebnismanipulation umfassend vermeiden, was bei der Blockchain-Technologie nicht zweifelsfrei gewährleistet ist.

Die Einführung eines elektronischen Patientendossiers gestützt auf das im April 2017 in Kraft getretene entsprechende Bundesgesetz betrifft vorläufig „nur“ die Digitalisierung von und den leichteren Zugang zu Informationen, ohne dass der Einsatz der Blockchain-Technologie vorgesehen ist.

Im Rahmen der Verwaltungsorganisation liesse sich die Blockchain-Technologie einsetzen, um die sichere und schnelle Kommunikation zwischen den Behörden und der Zivilgesellschaft zu verbessern, was aber voraussetzt, dass die Infrastruktur technologisch ohne grösseren Aufwand verwendbar ist. Bezug genommen wird in der Diskussion oft auf das E-Government-Programm in Estland und die Digitalisierung in Dänemark. Auch in diesen Ländern wird aber (z.B. für die E-Identität) meist nicht die Blockchain-Technologie eingesetzt. Hingegen ist Grossbritannien daran, mögliche Blockchain-Projekte zu analysieren, etwa im Steuerrecht und im Sozialversicherungsrecht.

In allen Anwendungsbeispielen ist aber im Auge zu behalten, dass die Infrastruktur dezentral ohne staatliche Kontrolle aufgebaut ist.

9.3.3 Register

Der Einsatz der Blockchain-Technologie ist an sich besonders geeignet für Registertätigkeiten. Blockchain selber funktioniert als Registerbuch, das die abgewickelten

Transaktionen verzeichnet und in der chronologischen Reihenfolge unveränderbar abspeichert. Einsatzmöglichkeiten der neuen Technologie stehen insbesondere im rein privatrechtlichen Bereich vor der Einführung, etwa mit Bezug auf die Nachverfolgung des Containerverkehrs bei der Hochseeschifffahrt sowie mit Bezug auf Produktion und Distribution von Nahrungsmitteln. Die Blockchain-Technologie lässt sich z.B. auch für den Herkunftsnachweis von Kunstgegenständen oder von Diamanten einsetzen.

Besondere Anforderungen an die Gewährleistung von Sicherheitsstandards sind indessen zu erfüllen, wenn Register auf Blockchain geführt werden sollen, die (auch) eine öffentliche Funktion haben. Diese Beurteilung gilt nicht nur für das Personenregister (künftige E-ID), sondern auch für das Handelsregister und das Grundbuch.

Die Führung des Handelsregisters auf der Blockchain-Infrastruktur würde die Kommunikation mit diesem erleichtern und die Effizienz im Verkehr erhöhen. Weil die Einträge im Handelsregister aber als „richtig" gelten und ihnen der gute Glaube zukommt (Art. 933 OR), muss zwingend die Zuverlässigkeit der Informationen gewährleistet sein. Angesichts dieser „Richtigkeitsgewähr" kommt der Staat nicht umhin, unter dem Aspekt der Informationssicherheit und der einwandfreien Geschäftsführung beim Betrieb von Blockchain zumindest in einer „Überwachungsfunktion" aktiv zu werden (s. Ziff. 9.1.3).

Ähnliche Vorteile hätte die Blockchain-Technologie für die Führung des Grundbuchs (Effizienz, Kostengünstigkeit). Aber auch das Grundbuch geniesst die Eigenschaft des öffentlichen Glaubens (Art. 971 und Art. 973 ZGB), was den Staat veranlassen muss, gewisse Kontroll- und Überwachungsaufgaben wahrzunehmen. Überdies wird die technologische Komplexität der Vorgänge erhöht, weil für die meisten Grundbucheinträge im Vorlauf ein notarieller Akt erforderlich ist; Effizienzgewinne würden also voraussetzen, dass auch elektronische notarielle Urkunden ausgestellt und auf die Blockchain des Grundbuchamtes übertragen werden könnten.

9.3.4 Private Organisationen

Vermehrt wird in letzter Zeit darüber diskutiert, organisationsinterne Vorgänge in Unternehmen auf Blockchain abzuwickeln. Die Rahmenbedingungen für elektronische Generalversammlungen, obschon vorläufig „nur" auf der Basis digitalisierter Informationen ohne Verwendung der Blockchain-Technologie, sollen in der anstehenden Aktienrechtsrevision geschaffen werden. Denkbar ist der Einsatz der Blockchain-Technologie auch im Rahmen des Accounting und des Reporting von Unternehmen bzw. allgemein bei der Ausgestaltung der Corporate Governance Anforderungen. Immerhin sind zusätzliche Herausforderungen für den Fall der Kommunikation mit Aufsichtsbehörden nicht zu übersehen (Stichwort „RegTech").

Noch kaum diskutiert ist bisher die Zulässigkeit von Gesellschaften, die ausschliesslich digital existieren. Die international-privatrechtlichen Staatsverträge sind auf solche Unternehmensformen nicht ausgerichtet, weil sich eine nur digital bestehende Organisation geographisch kaum lokalisieren lässt. Denkbar wäre für diesen Fall die Anknüpfung an die rechtlich relevanten Internetseiten, ähnlich wie im Verbraucherrecht, das oft vorsieht, dass Anbieter von Gütern oder Dienstleistungen auf der Internetseite ein Impressum oder eine legal Notice zu publizieren haben.

9.3.5 Transaktionen

a) Individuelle Verträge

Schon heute findet der Begriff der sog. Smart Contracts Verwendung. Von einem Smart Contract spricht man, wenn eine vernetzte und selbstausführende algorithmi-

sche Begründung von Vertragsbeziehungen zustande kommt; anstelle der Aushandlung des Vertragstextes wird auf bereits getroffene Vereinbarungen in einem Source Code (meist unter „Wenn-Dann-Bedingungen“) Bezug genommen. Kryptografische Protokolle legen die Vertragsbedingungen und die Zahlungsmechanismen fest. Eine persönliche Mitwirkung beim Vertragsabschluss ist nicht zwingend notwendig; im Falle einer intermaschinellen Kommunikation (wie sie z.B. beim IoT wegen der intelligenten Vernetzung von Gegenständen vorkommt), gibt die „Maschine“ (z.B. der Roboter) die Erklärung mit bindender Wirkung für deren Eigentümer ab.

Schwierigkeiten bei Smart Contracts treten auf, wenn für die Vertragsgültigkeit gesetzlich zwingend die Schriftform vorgesehen ist. Schriftlichkeit wird etwa für einzelne Konsumentenverträge verlangt, aber auch für Forderungsabtretungen (Art. 165 OR), was für den Aktienhandel relevant ist. Bei verlangter Schriftform sind die Bedingungen des ZertES 2003), die einen nicht unerheblichen technischen Aufwand verursachen und deshalb nicht leicht zu handhaben sind, einzuhalten.

Aus rechtssoziologischer Sicht eignen sich Smart Contracts (in der vollautomatisierten Abwicklung der Vertragsbeziehung) nicht für Situationen, in denen die Beachtung persönlicher Umstände erforderlich ist; eine individuelle Perspektive kann insbesondere im Kontext von Leistungsstörungen notwendig sein. Weiter stellen sich Probleme, wenn Meinungsverschiedenheiten zwischen den Parteien auftreten, die nicht durch eine im Programmcode schon enthaltene Vertragsanpassung gelöst werden können; in diesem Fall lässt sich über eine technologische Schnittstelle, welche die Blockchain mit der realen Welt verbindet (oft „Oracle“ bzw. „Orakel genannt), eine aussenstehende Schlichtungsstelle vorsehen.

b) Standardisierte Handelsgeschäfte

Grundsätzlich ist die Blockchain-Technologie gut geeignet für den Handel mit Wertpapieren, weil dafür oft nur Seriennummern, die eine rechtlich abgesicherte Identifikation ermöglichen, notwendig sind. Die zwingende Schriftlichkeit bei Abtretungen von Forderungen und bei Übertragungen von Wertrechten (Art. 165 und Art. 973c OR) verursacht aber die erwähnten technologischen Komplikationen (ZertES).

Eine mögliche rechtliche Alternative, um den standardisierten Handel auf Blockchain abzuwickeln, besteht darin, „colored Coins“ als Bucheffekten zu verstehen. Bucheffekten sind vertretbare Forderungs- oder Mitgliedschaftsrechte, die einem Effektenkonto gutgeschrieben sind und über welche die Kontoinhaber nach den Vorschriften des Bucheffektengesetzes vom 3. Oktober 2008 (BEG) verfügen können. Die Eintragung solcher Wertrechte erfolgt durch Verbuchung im Hauptregister einer Verwahrungsstelle; ein Betreiber hätte somit das Wertrechtebuch und das Hauptregister mittels Blockchain zu führen. Die Verfügung über Bucheffekten würde dann gestützt auf eine Weisung des Veräusserers, die formfrei gültig ist und auch konkludent erteilt werden kann, erfolgen.

c) Organisierte Handelssysteme

Nicht nur aus der Sicht der Marktteilnehmer, die standardisierte Transaktionen abwickeln, sondern auch für die Betreiber organisierter Handelssysteme erweist sich die Blockchain-Technologie als sinnvolle Infrastruktur.

Das Finanzmarktinfrastrukturgesetz vom 19. Juni 2015 (FinfraG) sieht organisierte Handelssysteme (Art. 42) und multilaterale Handelssysteme (Art. 26) vor. Während letztere für Blockchain-Transaktionen ungeeignet sind, weil alle Teilnehmenden reguliert sein müssen, ist bei den organisierten Handelssystemen die Abwicklung von

Transaktionen (Handel von Effekten und anderen Finanzinstrumenten) nach diskretionären Regeln möglich.
Weder müssen die Finanzinstrumente kotiert noch die Teilnehmenden reguliert sein: Der Betreiber des Handelssystems selber bedarf aber in der Regel einer Bewilligung als Effektenhändler.

Wenn die „colored Coins“ rein internetbasiert emittiert werden („Initial Coin Offering"), stellen sie Wertrechte dar (Art. 973c OR), weshalb sie – wie erwähnt – als Bucheffekten auszugestalten sind, damit sie sich als vertretbare Rechte einem Effektenkonto gutschreiben lassen können und der Kontoinhaber darüber verfügen kann (Art. 3 und 6 BEG). Die Zahlung lässt sich gleichzeitig durch eine virtuelle Währung auslösen. Einzelne Fragen zum Post-Trading und zum Clearing/Settlement bedürfen aber noch der rechtlichen Klärung. Die vorerwähnten Überlegungen gelten nicht nur für „traditionelle“ Finanzinstrumente, sondern ebenso sehr für „alternative“ Wertrechte oder Zertifikate, wie z.B. Rohstoff-, Edelmetall-, Energie- oder Klimawandelzertifikate.

9.4 Rechtliche Querschnittsmaterien

9.4.1 Blockchain und Datenschutz

Aus mehreren Gründen verursacht insbesondere die public Blockchain neue Herausforderungen für den Datenschutz. Die Stärken der public Blockchain liegen unbestritten in der Kombination der Unabänderbarkeit der Daten und eines Konsens- und Überprüfungssystems, das sich auf alle beteiligten Akteure abstützt. Ebenfalls geht das Design der public Blockchain davon aus, dass die eingestellten Daten richtig sind und deswegen integer bleiben müssen. Neue Blöcke können hinzugesetzt, nicht aber in der gleichen Blockchain nachträglich entfernt werden. Eine Gabelung der Blockchain (Fork) nach einer Änderung ist zwar möglich, unterläuft aber letztlich das Grundprinzip der Integritätssicherheit in der Blockchain. Dies steht in einem Spannungsverhältnis mit grundsätzlichen datenschutzrechtlichen Bestimmungen wie etwa dem Recht auf Vergessen, Berichtigung und Widerspruch. Die Blockchain-Forschung und der Datenschutz sind hier gefordert, neue Ansätze in der Privacy by Design zu finden, die dieses Spannungsverhältnis auflösen.

Bei einer genaueren Betrachtung ist festzuhalten, dass die Identität der Akteure bei Einträgen in die public Blockchain nicht hinreichend anonymisiert bzw. pseudonymisiert ist, um sie als nicht personenbezogene Daten einordnen zu können. Bereits der Transfer von Coins oder Tokens von einer Person zu einer anderen über Links wirft Fragen auf. Das Bundesgericht und der Europäische Gerichtshof haben IP-Adressen und sogar dynamische IP-Adressen als Daten eingeordnet, die eine Person hinter dem Anschluss erkennbar machen. Mittels der privaten und public Keys sowie der Hashwerte lassen sich die Identitäten über das Wallet bestimmen. Es ist davon auszugehen, dass aus einer objektiven Sicht der Aufwand heute nicht mehr derart gross ist, dass ein Akteur diesen nicht auf sich nehmen würde, womit die Bestimmbarkeit gegeben wäre.

Das Spannungsverhältnis zwischen Blockchain und Datenschutz könnte weiter zunehmen, je nach dem mit welchem Inhalt die zurzeit diskutierte EU Verordnung über Privatsphäre und elektronische Kommunikation (e-Privacy Verordnung im online-Bereich) ausgestaltet wird. Diese Verordnung könnte das Kriterium „Identifizierung“ durch „Singularisierung“ ersetzen“, d. h. bereits die Unterscheidbarkeit von anderen Personen und nicht die Identifizierung würde als Personenbezug gelten und grundsätzlich jede Kommunikationsinformation der Vertraulichkeit unterstellen. Schliesslich können

die Tokens etwa im Kontext des Registerrechts, des Gesellschafts- und Finanzmarktrechts und erst recht bei Wahlen direkt personenbezogene Daten beinhalten, welche das grundsätzlich auf Transparenz ausgelegte Blockchain-Design nicht vertraulich bearbeiten kann.

Blockchain stellt die Frage nach der örtlichen Anwendbarkeit der DSGVO und des DSG und nach den Folgen. Unter der Annahme, dass die private Blockchain personenbezogene Daten enthält, führt der extraterritoriale Geltungsanspruch der DSGVO dazu, dass strenggenommen alle Betreiber eines Blockchain-Knotenpunktes und sogar alle Miner als Verantwortliche oder Auftragsverarbeiter betrachtet werden müssten - und zwar weltweit, wenn die entsprechende Blockchain in der EU angeboten würde. Alle diese Verantwortlichen müssten alle Grundsätze des Datenschutzes, wie etwa die Einholung einer Einwilligung bei allen Blockchain-Nutzern, einhalten, was nicht praktikabel ist. Gesetzgebung, Aufsichtsbehörden und Technik stehen hier vor der Aufgabe, die Chancen von Blockchain zu wahren, ohne den Schutz der Privatsphäre und der informationellen Selbstbestimmung zu schmälern.

9.4.2 Haftungsrechtliche Fragen

Wie bei jeder neuen Technologie ergeben sich auch veränderte Verantwortungs- und Haftungsfragen. Im Einzelfall ist etwa zu beurteilen, in wessen Verantwortung ein „Fehler“ beim Einsatz der Blockchain-Technologie fällt, d.h. die Haftungszuordnungsproblematik ist zu regeln.

Eine weitere Herausforderung betrifft die Bewältigung der Anspruchssituationen im Falle der Konkurseröffnung über den Betreiber einer Blockchain-Infrastruktur. Weil die Betroffenen nicht wie im traditionellen Fall einzelne Güter aus der Konkursmasse herausverlangen, sondern vielmehr die Rückübertragung von Daten beanspruchen können, wird es unumgänglich sein, ein ausreichend abgesichertes Aussonderungsrecht in der Zwangsvollstreckung einzuführen (Anpassung des SchKG). Überdies sind die zivilprozessualen Vorschriften im Falle einer notwendigen Streitschlichtung neu auf die Besonderheiten der Blockchain-Technologie auszurichten.

Empfehlung:

43. Der Bund nimmt, unter Berücksichtigung der regulatorischen Entwicklungen im Ausland, die nötigen rechtlichen Anpassungen bei der Behandlung von digitalen „Datenpaketen“ (Tokens), von digital geführten Registern und im Bereich des Datenschutzes vor.

10 Analysefeld Digitale Aufklärung der Bevölkerung, Kompetenzaufbau, Mitgestaltung des Nutzers und Forschung

10.1 Ist-Zustand und weiteres Entwicklungspotenzial

In diesem Abschnitt sollen zuerst jene Prozesse, Faktoren oder Eigenschaften der Digitalisierung hervorgehoben werden, die im Zusammenhang mit der Sensibilisierung und Befähigung der Bevölkerung besonders relevant sind. Danach wird in Grundzügen der Zustand des Schweizer Bildungssystems im Hinblick auf digitalisierungsrelevante Aspekte beleuchtet.

10.1.1 Vier grundsätzliche Herausforderungen

1. Die erste Charakteristik der Digitalisierung ist die **beschleunigte Automatisierung** zahlreicher Prozesse in der Arbeitswelt. Die Automatisierung an sich ist kein neues Phänomen und hat bereits in der zweiten Hälfte des 20. Jahrhunderts in mehreren Wellen zu Umbrüchen beispielsweise in der industriellen Fertigung geführt. Es ist aber absehbar, dass die neuen digitalen Technologien einen zunehmend flexibleren Einsatz der Automatisierung ermöglichen und dass damit auch komplexere Abläufe von Robotern oder Software-Systemen übernommen werden können. Die konkreten Auswirkungen auf die Arbeitswelt sind schwierig vorauszusagen. Einige Studien sehen einen dramatischen Abbau von menschlichen Arbeitsplätzen voraus, während andere Studien dies mit Blick auf die bisherigen Erfahrungen deutlich relativieren. Gesamtgesellschaftlich gesehen hat die Beschäftigung in der Schweiz in den vergangenen Jahren trotz Automatisierungsschüben zugenommen, während sie in anderen Ländern zurückgegangen ist.

Unbestreitbar ist, dass ein Strukturwandel im Gange ist und ein Umbruch in der Art und Weise der Beschäftigung nicht vermeidbar ist. Genauso, wie der Fliessbandarbeiter durch Industrieroboter ersetzt worden ist, dürften in naher Zukunft klassische Tätigkeitsfelder wegbrechen und neue entstehen. Das stellt die grundsätzliche Frage, welche Art von Befähigung und Bildung der Bevölkerung vermittelt werden muss, um mit diesen Umbrüchen umgehen zu können. Art, Zahl, Anforderungen und Ausgestaltung der zukünftigen Jobs sind derzeit nicht absehbar. Die Digitalisierung dürfte viele Jobs anspruchsvoller machen, kann aber auch Instrumente liefern, die unterstützend wirken beispielsweise mittels augmented Reality (digitale Erweiterung der Realität).

Insgesamt jedoch resultiert aus der Digitalisierung die Herausforderung, dass die Notwendigkeit der Weiterbildung zunehmen wird; es gilt, die entsprechende Sensibilisierung für lebenslanges Lernen zu fördern und geeignete Angebote bereitzustellen.

2. Die zweite Charakteristik ist die **Quantifizierung aller Lebensbereiche**. Auch wenn gewisse Aspekte des menschlichen Lebens wie Liebe, Menschenwürde oder Vertrauen nie ganz in Zahlen gefasst werden können, ist inzwischen vieles mit Hilfe der heutigen technischen Möglichkeiten einfacher zu quantifizieren. Mobile Geräte zählen Schritte oder kontrollieren den Puls; digitale Fahrtenschreiber erfassen den Fahrstil von Menschen und Smart Meters detektieren Muster im Stromverbrauch. Diese „Quantifizierungsfreude“ wird verstärkt durch die Betonung von Werten wie Effizienz, Profitmaximierung und Leistungssteigerung, die in den meisten modernen Gesellschaften einen hohen Stellenwert einnehmen. Diese digitalen Vermessungs-Technologien erlauben es, auf individueller Ebene in bislang nicht gekanntem Ausmass das

„Selbst“ zu optimieren. Sie erhöhen entsprechend den Druck auf das Individuum, seine Effizienz und Leistungsfähigkeit mit anderen zu vergleichen.

Die durch die Digitalisierung vorangetriebene Quantifizierung vieler Lebensbereiche wirft die grundsätzliche Frage auf, wie das Bildungssystem auf diese neuen Möglichkeiten in Arbeitswelt und Privatleben reagieren soll. Insbesondere sollten Bürgerinnen und Bürger für Chancen und Risiken der Quantifizierung sensibilisiert werden. Denn diese „Selbstvermessung“ ist ambivalent – in manchen Fällen (z.B. bei chronischen Krankheiten) können Individuen ihren Lebensstil zum eigenen Wohl positiver gestalten, in anderen Fällen droht ein Konkurrenzkampf, dem man sich kaum entziehen kann, oder ein Burnout. Dies könnte insbesondere die Arbeitsmarktfähigkeit betreffen und hätte damit direkte Auswirkungen darauf, wie Arbeitskräfte künftig aus- und weitergebildet werden. Auch bei Organisationen und auf der Ebene des politischen Gemeinwesens sind positive und negative Effekte zu erwarten. So können beispielsweise Logistik, Verkehr und Energieverteilung optimiert und damit Umweltrisiken minimiert werden; doch können diese Organisationen durch solche Entwicklungen auch dazu verleitet werden, ihren Blick nur noch auf das Messbare zu lenken, sodass menschliche Entscheidungskompetenz zunehmend an Algorithmen abgegeben wird. Daraus können Probleme wie Diskriminierung oder Verminderung des menschlichen kreativen Potenzials entstehen. Diese werden im Kapitel „Ethik“ (s. Ziff. 11) angesprochen.

Bezüglich Sensibilisierung und Befähigung der Bevölkerung besteht die Herausforderung der Quantifizierung darin, ein genügendes Ausmass kritischer Reflexion zu fördern, damit Chancen und Risiken der durch die Digitalisierung vorangetriebenen Messbarkeit und „Algorithmisierung“ vieler Abläufe realistisch beurteilt werden können und ein verantwortungsvoller, selbstbestimmter Umgang mit ihnen möglich wird.

3. Das dritte relevante Charakteristikum ist die durch digitale Technologien enorm gestiegene **Möglichkeit, mediale Inhalte zu schaffen, zu verbreiten und zu verändern**. Medien wie z.B. der Buchdruck, Radio oder Fernsehen haben stark zu gesellschaftlichen Veränderungen beigetragen. Mittlerweile erlauben es moderne Kommunikationsnetze wie Internet und Mobilfunk sowie die zahlreichen damit verbundenen digitalen Technologien im Prinzip jeder Person, mediale Inhalte zu erzeugen und zu verbreiten. Gleichzeitig werden die Instrumente zur bewussten Manipulation medialer Inhalte immer raffinierter, und es ist absehbar, dass es immer schwieriger wird zu erkennen, ob gewisse Inhalte, Bilder, Videos oder Tonaufnahmen echt oder gefälscht sind. Die potentiell veränderten Inhalte sind bei der heutigen Informationsflut kaum zu erkennen. Beides steigert das Risiko, dass der Einzelne manipulierbar wird – nicht zuletzt auch deshalb, weil die Nutzung digitaler Medien auch Informationen über die Nutzerin oder den Nutzer selbst preisgibt, die zum Zweck der Beeinflussung (des Konsums, aber auch des Wahlverhaltens) genutzt werden können.

Klassische «Gatekeeper» im Informationsfluss wie beispielsweise Journalisten oder Musik- oder Videoanbieter finden sich in einer neuen Rolle wieder. Die ökonomischen Auswirkungen in Bereichen wie Presse, Film- und Musikwesen sind enorm.

Hinsichtlich Aus- und Weiterbildung stellt diese Entwicklung insbesondere die Medienfachleute vor neue Herausforderungen. Aber auch die Medienkompetenz der allgemeinen Bevölkerung ist gefordert. Die mit der Digitalisierung des Medienwesens einhergehenden Veränderungen finden sich auf allen Ebenen der Gesellschaft – von Phänomenen wie Cyber-Mobbing über das Auftreten neuer Medien-Akteure wie z.B. Produzenten populärer YouTube-Channels bis hin zur Beeinflussung demokratischer Prozesse durch digitale Propaganda, wie dies derzeit am Beispiel der US-Wahlen und des Brexit-Referendums untersucht wird. Diese Veränderungen bringen neue Probleme

mit sich. Die Nutzung sozialer Medien kann auch eine Suchtgefahr implizieren und durch Vereinzelung der Individuen den sozialen Zusammenhalt gefährden.

Die Herausforderung besteht folglich darin, die Bürgerinnen und Bürger mit der notwendigen Medienkompetenz auszustatten, um verantwortungsvoll mit diesen Instrumenten umzugehen. Dies betrifft in besonderem Masse auch Berufstätige im Bereich digitaler Medien.

4. Die vierte Charakteristik schliesslich besteht in einer **zunehmenden Abhängigkeit von autonomen Systemen**. In allen Lebensbereichen verwenden wir Computer, Internet und Smartphones. Auch wenn sich die heutige Zivilisation bereits in eine starke Abhängigkeit zur Technologie begeben hat, sind dennoch die Verbindungen und Abhängigkeiten zwischen den technischen Systemen noch weitgehend durch menschliche Kontroll-, Eingriffs- und Entscheidungsmöglichkeiten geprägt. Doch mit zunehmender Vernetzung physischer und virtueller Gegenstände (Internet of Things) und Verbreitung der KI nimmt die Abhängigkeit von autonom entscheidenden Systemen schnell zu. Das daraus resultierende Problem ist ein zunehmender Verlust an Entscheidungs-, Mitwirkungs- und Gestaltungsmöglichkeiten.

Dieser Verlust zeigt sich auch, wenn einzelne individuelle Entscheide über einen bestimmten Standard zu einer Situation führen, in welcher der Standard zwingend für alle anderen wird. In Rousseaus Worten käme es dann zu einer volonté de tous, aber nicht zu einer volonté générale, d.h. es käme zu einer Situation, in der individuelle Entscheidungen ohne Berücksichtigung der gesamtgesellschaftlichen Perspektive gefällt werden. Auch wenn man frei entscheiden kann, einen Standard anzuwenden oder nicht und damit zu einem Netzwerk zu gehören (eine Technik anzuwenden) oder nicht, kann man den Standard nicht selber verhandeln, und oft gibt es keine adäquaten Alternativen. Will man beispielsweise an einem Whatsapp Gruppenchat teilnehmen, muss man die entsprechenden Nutzungsbedingungen akzeptieren. In vielen Fällen bedeutet das, dass über die Nutzerinnen und Nutzer Daten gesammelt werden, mit denen oft auch künstliche Intelligenzsysteme betrieben werden. Diese Systeme lernen damit unser menschliches Verhalten. Dank der enormen Datenmenge können die Maschinen aber auf weit mehr Erfahrungen zurückgreifen als es ein Mensch je kann. Die Besitzer intelligenter Maschinen können damit über andere Macht ausüben. Die Nutzer können sich dem weder effektiv widersetzen noch werden sie angemessen aufgeklärt. Von informiertem Einverständnis kann also keine Rede sein. Unrealistische Hoffnungen wie „die Wirtschaft wird schon von selber gute Lösungen hervorbringen“ könnten Staat und Bevölkerung davon abhalten, die für sie besten Bedingungen einzufordern.

Die grundsätzliche Herausforderung bezüglich Sensibilisierung und Befähigung der Bevölkerung ist es, die Menschen zu befähigen, ein ausreichendes Mass an menschlicher Kontrolle und Entscheidungsfähigkeit zu haben, damit sie nicht nur «funktionelle Einheiten» in einem komplexen soziotechnischen System werden, was mit Menschenwürde nicht vereinbar wäre (s. den Abschnitt über Ethik).

10.1.2 Gegebenheiten des Schweizer Bildungssystems

Es ist angesichts der heutigen Entwicklung unabdingbar, dass die Bevölkerung sensibilisiert und befähigt werden muss, gesellschaftliche Veränderungen im Zusammenhang mit der Automatisierung, Quantifizierung, Medialisierung und zunehmenden Abhängigkeit als für sie relevant zu erkennen und mitzugestalten. In erster Linie sind hier Bildungssystem und Medien gefordert. Unter Bildungssystem ist dabei die Gesamtheit aller Bildungsinstitutionen wie Volksschule, Mittelschule, Hochschule, Berufsbildung, Volkshochschule und Weiterbildung zu verstehen. Bezüglich der Formulierung von Empfehlungen müssen dabei zwei Gegebenheiten berücksichtigt werden:

Erstens ist im Schweizer Bildungssystem eine Vielzahl von Akteuren aktiv mit ihren jeweils eigenen Auffassungen, wie das Bildungssystem auf die Herausforderungen der Digitalisierung reagieren soll. Dies führte in den vergangenen Jahren zu zahlreichen Reformvorschlägen im Bildungsbereich, die zu einer gewissen Reformmüdigkeit bzw. auch zu einer Reformüberdosis geführt haben – insbesondere bei den Lehrkräften. Zudem findet man in der Schweiz nicht schnell Mehrheiten für Veränderungen in der Grundausbildung. Bei allen Vorschlägen, die das Bildungswesen betreffen, sollte diesen Problemen Rechnung getragen werden.

Zweitens ist in der Schweiz der Grossteil des Bildungswesens kantonal organisiert. Dies erschwert ein kohärentes Vorgehen. Dennoch ist dieser Sachverhalt insofern positiv zu werten, als dass dadurch Experimentierraum gegeben und Vielfalt möglich ist. Die folgenden Empfehlungen sind denn auch als Anstoss zu verstehen, diese Vielfalt an Möglichkeiten zu nutzen, sodass angesichts der hohen Unsicherheit über die künftigen Entwicklungen und Anforderungen ein breites Portfolio an Massnahmen aufgebaut werden kann.

10.2 Möglichkeiten und Grenzen

Das Ziel der Sensibilisierung, Befähigung und Bildung der Bevölkerung ist „digital Literacy" - also Fähigkeiten und Kompetenzen, um die Chancen der Digitalisierung verantwortungsvoll nutzen und den Herausforderungen adäquat begegnen zu können. Unter „digital Literacy“ ist alles zu verstehen, was die Möglichkeit und Fähigkeit der Bürgerinnen und Bürger erhöht, in einer digitalen Welt erfolgreich zu leben. Das bedeutet aber nicht, dass man alle Herausforderungen der Digitalisierung mittels Bildung gewissermassen auf die einzelne Person abschieben kann. Gewissen Problemen ist nicht durch „digital Literacy", sondern durch geeignete Gesetze zu begegnen, die z.B. Anbietern digitaler Dienstleistungen gewisse Pflichten aufbürden. Zum Vergleich: Die Tatsache, dass Menschen durch allgemeine Verkehrserziehung und spezifische Ausbildungen (z.B. Fahrprüfung) zu verantwortungsbewussten Verkehrsteilnehmern ausgebildet werden, heisst nicht, dass es keine öffentlichen Massnahmen für Verkehrssicherheit und Umweltschutz braucht. Vielmehr sorgen Gesetze und behördliche Vollzugsmassnahmen dafür, dass Hersteller und Verkäufer von Fahrzeugen ihre Pflichten erfüllen.

In Bezug auf die formulierten Herausforderungen bedeutet dies folgendes.

10.2.1 Beschleunigte Automatisierung

Es besteht Konsens, dass die Digitalisierung tiefgreifende gesellschaftliche Auswirkungen haben wird. Wie erwähnt, ist es schwierig abzuschätzen, wie sich die Beschäftigung entwickeln wird. Es scheint darum ratsam, in Szenarien zu denken, um auch für den Fall einer wachsenden und gegebenenfalls hohen Arbeitslosigkeit vorbereitet zu sein. Bedingt durch die Veränderungen wird sich das Tätigkeitsprofil von Menschen zudem mehr in Richtung soziale, umweltbezogene und kreative Tätigkeiten verschieben. Das erfordert einen Übergang von standardisierter hin zu personalisierter Ausbildung. Die beschleunigte Automatisierung bringt auch neue Formen der Zusammenarbeit zwischen Mensch und Maschine (KI) hervor und durch KI moderierte Zusammenarbeit zwischen Menschen. Als Folge dessen sollte sich die Ausbildung auch damit auseinandersetzen, wie Mensch und KI zusammenarbeiten können.

10.2.2 Quantifizierung aller Lebensbereiche

Rund um das Thema Quantifizierung aller Lebensbereiche ist vom Grundsatz auszugehen, dass die technischen Möglichkeiten und Hilfsmittel nur Werkzeuge sind, niemals Selbstzweck. Zudem soll als oberstes Prinzip gelten, dass die Bürgerinnen und Bürger souverän über die Verwendung ihrer Daten entscheiden können. Daraus folgt erstens, dass informationelle Selbstbestimmung möglich und dass zudem die Vermessung von Bürgerinnen und Bürgern durch private und öffentliche Entscheidungsträger beschränkt sein muss. Dieser Aspekt ist vorab auf gesetzgeberischer Ebene zu regeln und fällt damit nicht direkt in den Bereich Bildung. Zweitens ist sicherzustellen, dass die zunehmende Nutzung von Algorithmen bei der Bearbeitung der erhobenen Daten zum Zweck von Entscheidungsunterstützung oder gar automatisierten Entscheidungen grundlegende Werte nicht verletzt; die Algorithmen sollen kurz gesagt nicht manipulieren oder diskriminieren, sondern fair und nachhaltig sein. Dies erfordert insbesondere Massnahmen auf der Ebene der beruflichen Aus- und Weiterbildung jener Spezialisten, welche Algorithmen entwickeln und einsetzen. Grundlagen in werte-sensitivem Design (s. auch Ziff. 11) sollten demnach ein obligatorisches Element im Berufsbild von Software-Ingenieuren werden. Ausserdem ist beim Einzelnen das Bewusstsein für unbeabsichtigte und negative Nebenwirkungen selbstbestimmter Vermessung zu schärfen. Dieser Punkt könnte ein inhärentes Element einer „digitalen Grundausbildung" sein, die Teil der schulischen Ausbildung aller sein sollte.

Bei der Entwicklung der entsprechenden Lehrpläne und -mittel für die schulische und berufliche Aus- und Weiterbildung ist dabei auf das grundlegende Motiv für die Quantifizierung hinzuweisen. Vermessung impliziert zunehmende Kontrolle unter dem Primat der Effizienz. Doch wenn alles optimiert wird, wird Innovation behindert. Gerade in kreativen Prozessen (beispielsweise in der Wissenschaft) findet Fortschritt oft durch Zufall und durch Trial and Error statt. Fehler können zu entscheidenden Einsichten führen und wichtig für den Fortschritt sein. Ausserdem weiss man oft nicht im Vornherein, was künftig wichtig sein wird.

Zu starke Quantifizierung und Algorithmisierung von Abläufen schränken nicht nur individuelle Freiräume ein. Sie unterminieren auch Nonkonformismus, Diversität und Querdenken, die für Lernprozesse und gesellschaftliche Krisenfestigkeit wichtig sind. Das bedeutet, dass Ineffizienz und Ermessensspielräume bis zu einem gewissen Grad akzeptiert werden sollten. Die dadurch geschaffenen Entscheidungsfreiräume ermöglichen Diskussionsräume, Reflexionsmomente und neue Handlungsspielräume. Im Grundsatz bedeutet dies, dass Quantifizierung als Instrument der (Selbst-)Reflexion von Einzelnen oder Institutionen positiver zu bewerten ist als deren Einsatz zum Zweck der Bewertung und Selektion.

Es ist den Bürgerinnen und Bürgern ausserdem bewusst zu machen, dass auch die selbstbestimmte Preisgabe von Informationen andere in Zugzwang bringen kann. Erwähnt eine Frau beispielsweise im Bewerbungsgespräch, dass sie keine Kinder haben kann oder will, erhöht sie damit zwar möglicherweise ihre Chance, die Stelle zu bekommen. Dieses Verhalten kann aber dazu führen, dass andere Frauen durch das Nichtansprechen dieses Themas einen Nachteil erlangen, weil die blosse Nichterwähnung zu einer möglichen Information wird. Schliesslich ist auch festzuhalten, dass sich immer auch die Frage der Korrektheit und Relevanz der erfassten Daten sowie der Gültigkeit der Modelle, anhand derer die Daten ausgewertet werden, stellt. Um Freiheiten nicht einzuschränken, sollten demnach gewisse Daten nicht erhoben oder nicht verwendet werden. Welche Daten das genau sind, muss Gegenstand eines gesellschaftlichen Reflexionsprozesses sein, der durch eine Vielzahl von Massnahmen unterstützt werden kann.

Im Weiteren ist festzuhalten, dass auch Lern- und Bildungsprozesse zunehmend Gegenstand der Quantifizierung werden. Je mehr Bildung digital vermittelt wird, desto mehr kann der Lernprozess selbst vermessen werden: Wie oft man auf Lerninhalte zugreift, wie lange man für das Lesen bestimmter Texte braucht, wie viele Fehler man beim Schreiben einer Antwort macht, und vieles mehr kann erfasst und ausgewertet werden. Dies mag für das Identifizieren spezifischer Lernschwächen hilfreich sein – gleichzeitig wirft es aber viele Folgefragen auf: Wie verändert sich das Lernen, wenn jeder Lernschritt vermessen und in aggregierter Form dem Lernenden oder möglichen Arbeitgebern gemeldet wird? Was bedeutet dies für die Rolle der Lehrerin oder des Lehrers? Wem gehören die während des Lernens erhobenen Daten, dem Studierenden oder der (Hoch-)Schule? Dürfen Selektionsentscheide anstelle von Prüfungen auf das „Lernprofil" eines Lernenden abgestützt werden? Was bedeutet es für den Stellenwettbewerb, wenn anstelle eines bewusst gestalteten CV die „Lern-Analytik" einer Person bei einer Bewerbung eingereicht wird? Solche Fragen müssen verstärkt in den Fokus der pädagogischen Forschung rücken, um unbeabsichtigte Effekte wie z.B. neue Formen von Diskriminierung zu verhindern.

Schliesslich ist auch die Bedeutung der zunehmend verfügbaren Daten und Algorithmen für den Bildungsprozess selbst zu klären. Datensätze mit grossem Potenzial für gesellschaftliche Innovationen (z.B. anonymisierte Daten von Bewegungsmustern von Fahrzeugen oder Daten über den Stromverbrauch) sollten – selbst wenn sie von privaten Unternehmen erhoben worden sind – unter geeigneten Umständen frei verfügbar gemacht werden (z.B. anonymisiert, aggregiert). Es wird von den individuellen Fällen abhängen, wie diese Umstände genau auszugestalten sind. Neue Ansätze wie „Open Data", „Open Source", „Open Access", „Open Science" und „Open Innovation" bieten das Potenzial zur kombinatorischen Innovation. Wenn Schüler, Lehrende, Studierende oder Berufsleute in Weiterbildung darauf zugreifen können, können sie mit neuen Ideen experimentieren und so selber Innovationen vorantreiben. Heutzutage wird solchen offenen Ansätzen und Citizen Science eine grosse Bedeutung beigemessen. Allerdings ist auch hier zu betonen, dass nicht alle Daten offengelegt werden können, beispielsweise aus Gründen der Privatsphäre oder der Sicherheit. Jedoch könnten bei Datenanalysen das zugreifbare Datenvolumen und der freigeschaltete Funktionenumfang abhängig gemacht werden von Qualifikation, Reputation, Fairness und Verantwortlichkeit der Datennutzung, und dies bei gleichen Zugangschancen für alle.

10.2.3 Medienbildung

Medienbildung hat sich in den vergangenen Jahren zu einem unbestrittenen Element der digitalen Bildungsoffensive entwickelt. Wichtige Elemente dabei sind die Vermittlung von Grundkenntnissen über Informationsverarbeitung und -nutzung, über Medientechnologien und die individuellen und gesellschaftlichen Folgen ihrer Nutzung, über die kulturstiftende Wirkung von Medien und die Möglichkeiten ihrer kreativen Nutzung und Gestaltung. In inhaltlicher Hinsicht bedeutet dies eine Förderung der Fähigkeit, relevante Informationen zu finden und kritisch zu bewerten, Informationen zu kuratieren und neues Wissen zu produzieren. Die Vermittlung der Fähigkeit, problematische Aspekte digitaler Medien wie Fake News, Sucht(potential) oder Cyber-Mobbing zu bewältigen, ergänzen die oben genannten Elemente. Medienbildung verlangt entsprechende Anpassungen sowohl in den Lehrplänen als auch der Lehrerbildung, was an vielen Orten bereits angelaufen ist.

Ein besonderes Augenmerk ist auf die Aus- und Weiterbildung der Medienschaffenden selbst zu richten. Angesichts der tiefgreifenden Transformation der Medienbranche durch die Digitalisierung ist auch hier das Bewusstsein gereift, dass die entsprechenden Fachleute vertieft in den erwähnten Kompetenzen geschult werden müssen. Diese

bereits laufenden Anstrengungen sind zu unterstützen, was auch die Schaffung neuer Berufsbilder, wie z.B. Datenjournalisten beinhalten kann. Ein Fokus sollte dabei auch die (technische) Schulung sein, digitale Fälschungen aller Art besser erkennen zu können. Angesichts der wachsenden Manipulationsmöglichkeiten ist absehbar, dass sich im digitalen Bereich neue „Gate Keepers“ herausbilden könnten, die die Qualität und Glaubwürdigkeit der vermittelten Informationen garantieren.

10.2.4 Zunehmende Abhängigkeit

Mit zunehmender Vernetzung physischer und virtueller Gegenstände (Internet of Things) und Verbreitung der KI nimmt die Abhängigkeit von autonom entscheidenden Systemen schnell zu. Bei aller Autonomie der Systeme sollte es klare Verantwortlichkeiten geben, die auch zur Rechenschaft gezogen werden können. Zudem soll der Mensch idealerweise mindestens noch eine Kontrollfunktion im Prozess wahrnehmen können. Drohende Kontrollverluste sollte man zudem antizipieren und sich Gedanken machen, wie man ihnen begegnen kann. Als Beispiele solcher Regressmassnahmen dienen das Aussetzen des Handels oder die Ungültigklärung und Rückabwicklung bei Flash Crashes (starke plötzliche Kurseinbrüche an den Finanzmärkten). Einem drohenden Kontrollverlust beim Datensammeln könnte man begegnen, indem man eine differenzielle Privatsphäre anwendet. Dabei würde man die Daten so bearbeiten, dass die Einzelperson nicht mehr erkennbar ist und ihre Privatsphäre geschützt ist. Dies könnte auch bei Weiterverkauf oder Weitervergabe der Daten angewendet werden. Schliesslich gilt es die Mitbestimmung des Einzelnen im Rahmen des Möglichen zu unterstützen. Standards wie Kompatibilität, Offenheit und Formbarkeit (Mitbestimmung) könnten hier auch zur Anwendung kommen. Allgemein besteht hier aber am wenigsten Spielraum für die Sensibilisierung und Befähigung der Bevölkerung.

Es herrscht Einigkeit, dass aufgrund des digitalen Wandels in der Berufswelt zunehmend andere Kompetenzen gefragt sein werden als früher. Bestimmt werden IKT-Kompetenzen gefragt sein. Die Kernkompetenz ist hierbei das sogenannte computational Thinking (vgl. Ziff. 4.3.3), d.h. „die individuelle Fähigkeit, eine Problemstellung zu identifizieren und abstrakt zu modellieren, sie dabei in Teilprobleme oder -schritte zu zerlegen, Lösungsstrategien zu entwerfen und auszuarbeiten und diese formalisiert so darzustellen, dass sie von einem Menschen oder auch einem Computer verstanden und ausgeführt werden können“[15]. Den Zugang zu dieser Kernkompetenz erhält man u.a. durch die Anwendung einer Programmiersprache und das Programmieren eines Computers oder durch Zusammenarbeit mit künstlicher Intelligenz. Dies kann in der Schule, z.B. durch die Erstellung von einfachen Computerspielen oder die Programmierung von simplen Robotern den Kindern einfach vermittelt werden.

Eine Fixierung oder Einschränkung auf IKT ist aber nicht zielführend. Es werden noch andere Kompetenzen wichtig sein. Jede Bildungsstufe wie Volksschule, Mittelschule, Hochschule, Berufsbildung, Volkshochschule und Weiterbildung könnte – sofern dies nicht schon erfolgt ist - unter Einbezug aller Anspruchsgruppen die Kompetenzen formulieren, die nötig sind, um mit den vier oben genannten (und allfälligen anderen) Herausforderungen umzugehen.

Es wird hier kein Kanon der zukünftig nötigen Kompetenzen formuliert; dieser Anspruch übersteigt die Möglichkeiten des hier vorgelegten Berichts. Ein solches Ergebnis sollte bottom-up erarbeitet werden unter Einbezug aller betroffenen Akteure (inkl.

[15] https://www.nzz.ch/feuilleton/soll-der-mensch-wie-ein-computer-denken-ld.1292090, [Stand 20. Februar 2018].

Auszubildende und Lehrkräfte). Nachfolgend sind einige exemplarische Kompetenzen skizziert, die hilfreich sein können, die genannten Herausforderungen zu meistern:

Die beschleunigte Automatisierung erfordert, dass alle befähigt werden, diese zu verstehen, schnell dazu zu lernen und sich flexibel an neue Chancen und Notwendigkeiten anzupassen. Das bereits genannte computational Thinking ist hierfür eine Schlüsselkompetenz. Zudem werden die Fähigkeiten wichtig, Wissen zu teilen, mit anderen zu kooperieren und Dienstleistungen und Produkte gemeinsam zu kreieren. Kreative Fähigkeiten sowie soziale und Umwelt-Kompetenz werden ebenfalls an Bedeutung zunehmen. Nützlich sein werden ebenso die Fähigkeiten, autonom und kritisch zu denken (critical Thinking), also bewusstes und selbstgesteuertes Denken, das Analyse, Interpretation oder Bewertung und Schlussfolgerung beinhaltet, sowie sich länger auf eine Tätigkeit zu konzentrieren, genauso wie handwerkliche Fähigkeiten.

Im Zusammenhang mit der Quantifizierung aller Lebensbereiche wird ein kompetenter Umgang mit Daten im weiteren Sinn wichtig werden (d.h. was Daten sind, wie sie verarbeitet werden, wie die Resultate zu interpretieren sind und welche Ungewissheiten mit ihnen verbunden sind). Ein vertiefendes Verständnis des Begriffs der Wahrscheinlichkeit sowie Wahrscheinlichkeitsrechnen dürften für die Grundausbildung aller wichtiger werden.

Bei der Medienbildung könnten gesellschaftliche, ethische, juristische oder wirtschaftliche Implikationen des digitalen Wandels oder des „digital Divide" thematisiert werden, ebenso die Themen Datenschutz, Privatsphäre, Menschenrechte und Menschenwürde und der Umgang mit Fake News. Reflexionsfähigkeit, die Fähigkeit, relevante Informationen zu finden und kritisch zu bewerten, Informationen zu kuratieren und neues Wissen zu produzieren sind ebenfalls bedeutsam.

Um auf die durch die zunehmende Abhängigkeit aufgeworfenen Herausforderungen reagieren zu können, wird zudem ein Grundverständnis von Informationsverarbeitung wichtig sein, nebst der Möglichkeit der kreativen (Mit-)Gestaltung im digitalen Zeitalter und der Arbeit in interdisziplinären Teams. Weiter könnte es wichtig werden, ein Verständnis dafür zu entwickeln, dass Informationssysteme sozio-technische Systeme sind, d.h. dass IKT-Systeme gesellschaftliche Implikationen haben und Veränderungen bewirken (auch unbeabsichtigte) sowie dass in IKT-Systemen explizit oder implizit ein Wertesystem eingebaut ist.

Unabhängig davon, welche Kompetenzen gefragt sein werden, werden wir ein Leben lang lernen. Im digitalen Zeitalter befinden wir uns in einer lernenden Informations-Gesellschaft, und es erscheint daher wünschenswert, wenn lebenslanges Lernen einen hohen Stellenwert bei allen erhält. Mit lebenslangem Lernen sind klassische Weiterbildungskurse, selbstständiges Lernen mit Fachliteratur, Lernen am Arbeitsplatz, E-Learning, Lernen in Gruppen, über kulturelle Veranstaltungen, bei der Rezeption von Medien[16]),Lernen mit Hilfe von MOOC („Massive Open Online Courses"), Lernen im Fablab oder Maker Spaces gemeint.

10.3 Erkenntnisse

Um die Bevölkerung zu sensibilisieren und zu befähigen, sind die Bildung, die Kultur und die generelle Öffentlichkeit die geeigneten Kanäle. Für die Bildung wird dabei vom Schweizerischen Bildungssystem ausgegangen.

[16] https://www.nzz.ch/wissenschaft/bildung/weiterbildung--gebot-oder-fluch-der-zeit-1.18179900 [Stand Oktober 2017].

10.3.1 Obligatorische Schule und die Allgemeinbildung bis zur Tertiärstufe

Für die obligatorische Schule und die Allgemeinbildung bis zur Tertiärstufe muss unter Einbezug aller Beteiligten ein stufengerechter Kanon darüber erarbeitet werden, welche Grundkompetenzen für die Bewältigung des digitalen Wandels gefragt sind. Dieser muss regelmässig überdacht und aktualisiert werden. Die genaue Ausgestaltung der Vermittlung „digitaler Grundfertigkeiten" soll das ganze Spektrum des menschlichen Lernens umfassen und sich nicht auf Lernen mittels Computer beschränken.

Die EDK soll die verschiedenen kantonalen Bildungsräume für Experimente nutzen und einen Austausch und gegenseitiges Lernen fördern. Folgende Anregungen können dabei Beachtung finden:

- Wissen über digitalisierungsrelevante Aspekte sollte genderneutral und unter Einbezug unterschiedlicher Bildungshintergründe vermittelt werden.[17]
- Die Bestrebungen zu einem elektronischen Bildungsdossier sind zu begrüssen. Dabei ist es notwendig, dass die informationelle Selbstbestimmung über die Daten in den Händen der Auszubildenden bleibt (für die Arbeitswelt gilt analoges für die Arbeitnehmer). Die Expertengruppe empfiehlt, das individuelle Lernverhalten sparsam zu quantifizieren und nicht zu transparent zu machen. Dies sollte in der Revision des DSG berücksichtigt werden.
- Es ist ein Weg zu finden, um mit der Diskrepanz zwischen der Rasanz der (Kompetenz-)Entwicklung und der Langsamkeit der demokratischen Prozesse umzugehen, damit Entscheidungen bezüglich der Ausgestaltung des Bildungssystems (Lehrpläne, Kompetenzen, etc.) zeitgemäss bleiben.
- Denkbar wäre die Förderung von Vorreiterschulen, die Spielraum für die experimentelle Prüfung neuer Lehrformen und -inhalte erhalten. Dies könnte z.B. weniger Frontalunterricht und Arbeit von Schülerinnen und Schülern an eigenen Projekten in Coworking Spaces oder Unterrichten nach dem Modell des „flipped Classroom“ (Informationsaneignung durch begleitetes Selbststudium) beinhalten. Solche Vorreiterschulen könnten sich zu einer Art lernender Organisation entwickeln, welche Orientierungspunkte für Bildungspolitik und -verwaltung, für andere Schulen oder Pädagogische Fachhochschulen generieren.
- Gerade in der Grundbildung, wo man, wie erwähnt, nicht schnell zentral gesteuerte Veränderungen auf der Strukturebene einführen kann, sind Lehrkräfte und Schulleitungen entscheidende Akteure. Sie sollen motiviert, ermutigt und befähigt werden, Auszubildende für die Digitalisierung „fit“ zu machen. Damit ist auch die Ausbildung der Lehrkräfte entscheidend: Es braucht Personal, das digital kompetent und souverän ist, eigene Lösungen zu entwickeln, und das genügend Freiräume und Zeit hat. Es braucht zudem auch entsprechende Lehrmittel (z.B. für Medienbildung oder für digitale Techniken wie Programmieren oder Robotik).
- Es wäre denkbar, dass auch auf tieferer Stufe vermehrt Projektarbeiten durchgeführt werden (etwa mit 3D-Druckern). Vorstellbar wäre auch, dass externe Praktiker, Experten oder Informatikstudierende zum Unterricht beitragen.

[17] https://ictswitzerland.ch/media/dateien/Bildung/ICTswitzerland-Positionspapier-Frauen_staerken_die_Informatik.pdf [Stand März 2018]; https://ictswitzerland.ch/publikationen/attraktivitaet-von-ict-berufen/ [Stand März 2018].

- Kinder und Jugendliche haben oft einen rascheren Zugang zu digitalen Technologien, d.h. Lehrkräfte könnten auch von den Auszubildenden lernen. Co-Learning sollte daher gefördert werden.
- Es ist zu überprüfen, ob der Leistungsbewertung eine weniger wichtige Rolle zukommen sollte. Motivation, Kreativität, Neugier und Zusammenarbeit der Auszubildenden sollte eine wichtigere Rolle spielen.
- Personalisierter Unterricht und individuelle Talentförderung, aber auch Charakterbildung und kollektive Intelligenz sind (weiter) zu fördern.
- Man könnte darüber nachdenken, wie experimentelle Freiräume und/oder digitale Wahlfächer an Schulen eingebaut werden könnten.
- Fablabs oder Makerspaces könnten neue Lehr- und Lernformen sein; z.B. wäre in dieser Form ein moderner, digitaler und kreativer Werkunterricht denkbar.
- Bei der Ausgestaltung und Nutzung der Schulgebäude sind neue Lehr- und Lernformen zu berücksichtigen.
- Die Umsetzung der Kompetenzen im Bereich Medien und Informatik sollte eine hohe Priorität geniessen.
- Der Bund könnte überprüfen, ob er weiter mit dem Business Modell „Verlage“ arbeiten will, oder wo „open educational Resources" (freie Lern- und Lehrmaterialien mit einer offenen Lizenz) eine Alternative sind.
- Das Bildungsmonitoring soll überprüfen, ob die im Lehrplan 21 formulierten Kompetenzen zum Bereich Medien und Informatik erreicht werden.
- Der Bund könnte die educa.ch mit Kompetenzen und Finanzen stärken (ähnlich dem Projekt „E-Government“), um deren Innovationspotential zu vergrössern.
- Der Bund stellt sicher, dass wichtige Aspekte des digitalen Bildungsraums in den gemeinsamen bildungspolitischen Zielen ihren Niederschlag finden.
- Die Pädagogischen Hochschulen kümmern sich darum, dass die neuesten Erkenntnisse im Bereich digitale Bildung in die Lehreraus-und -fortbildung einfliessen.

10.3.2 Hochschulen

An den Schweizer Hochschulen fehlt ein „Studium Digitale“ (analog einem Studium Generale). Dieses sollte ins Curriculum aufgenommen werden. Ebenfalls sind die internen Strukturen für die interdisziplinäre Zusammenarbeit ungenügend und müssen gestärkt werden, wobei den individuellen Profilen der Hochschulen Rechnung getragen werden soll.

Folgende Anregungen können bei der Umsetzung dieser Grundempfehlungen Beachtung finden:

- Das genannte „Studium Digitale" soll nicht nur digitale Kompetenzen (u.a. computational Thinking) und Grundkenntnisse zu Cybersecurity vermitteln, sondern auch für die Bewertung der Digitalisierung der Gesellschaft relevantes Wissen humanistischer Fächer (geschichtliche, gesellschaftliche, ökonomische, philosophische, ethische und rechtliche Aspekte).

- Digitale Lernformen wie MOOC (Massive Open Online Courses), interaktive virtuelle Welten oder Plattformen für personalisiertes Lernen sollen vermehrt Anwendung finden, wobei die Studierenden die Kontrolle über die so generierten Daten über das eigene Lernverhalten behalten sollten.
- Durch öffentliche Mittel geförderte Forschung soll die dabei erzielten Erkenntnisse (Daten, Publikationen) soweit möglich offen zugänglich machen (Open Access); Formen der Einbindung von wissenschaftlichen Laien in den Forschungsprozess (Citizen Science) sind zu fördern.
- Für den Wissenstransfer sollten unternehmerische Kompetenzen von Studierenden sowie universitäre Start-ups gefördert werden. Experimentierräume und Plattformen sollen es auch den KMU ermöglichen, einfacher auf universitäres Wissen und Kenntnisse zuzugreifen.
- Wie bereits der Lehrkörper auf unterer Stufe, sollten auch die Professorinnen und Professoren motiviert, ermutigt und befähigt werden, sich „digital fit" zu machen und entsprechend weiterzubilden sowie mit neuen Möglichkeiten zu experimentieren und diese zu erforschen.
- Es sollten neue Finanzierungsmodelle für die Forschung erprobt werden. Man könnte beispielsweise in gewissen Bereichen nicht basierend auf Projekteingaben Geld sprechen, sondern basierend auf Resultaten und deren Impact (sog. Refunding). So könnten jene belohnt werden, die (schnell) relevante Resultate zu wichtigen Themen hervorbringen.
- Zentrale Elemente für die verantwortliche Gestaltung des digitalen Wandels sind durch entsprechende Forschungsprogramme oder -zentren zu unterstützen, beispielsweise im Bereich digitale Ethik und werte-sensitives Design.

Empfehlung:

44. Bund und Kantone sorgen dafür, dass die Schülerinnen und Schüler im Rahmen der obligatorischen Schule und alle Studierenden die notwendigen Grundfertigkeiten und Kompetenzen für den Umgang und die Gestaltung mit digitalen Technologien und der Transformation entwickeln.

10.3.3 Berufliche Aus- und Weiterbildung

In der Schweiz fehlen die Strukturen, die ein lebenslanges Lernen für die Berufsleute aller Bereiche erleichtern. Es gilt insbesondere zu überlegen und auszuhandeln, wer für lebenslanges Lernen zuständig ist, wer es bezahlen soll, wie man es in der heutigen Situation umsetzen und finanzieren kann und welche Anreize (z.B. Steuererleichterungen, Stipendien, bezahlte Weiterbildungstage) man setzen könnte.

Folgende Anregungen könnten dabei Beachtung finden:

- Berufsleute aller Bereiche könnten ein lebenslanges „Bildungskonto" erhalten, das Unterbrüche in der beruflichen Karriere ermöglicht, um neue Fähigkeiten zu erlernen. Gewisse, bereits bestehende Lenkungsabgaben könnten für die Finanzierung eingesetzt werden.
- Berufsleute aller Bereiche sollten Grundkenntnisse im Bereich Cybersecurity erhalten, die modular für die spezifischen Bedürfnisse einzelner Berufsgruppen erweitert werden können. Dabei kann auf bereits bewährte Materialien zur Förde-

rung der IKT-Sicherheit in Unternehmen und Behörden auch aus dem angrenzenden Ausland (D, A, F, I) im Hinblick auf die rasche Verfügbarkeit und unter Berücksichtigung unserer Landessprachen zurückgegriffen werden.[18]

- Bei der Informatikausbildung sollte vermittelt werden, dass die Entwickler auch die ethischen, sozialen, ökonomischen, kulturellen, rechtlichen, und gesellschaftlichen Implikationen bedenken sollten. Algorithmen-Designer müssen lernen, dass die Folgenabschätzung zu ihrer Arbeit gehört, und lernen, diese durchzuführen.
- Alle Medienfachleute sollten spezifisch und unter Berücksichtigung entsprechender technischer und forensischer Kenntnisse zur Sicherung der Vertrauenswürdigkeit digitaler Medien ausgebildet werden.
- Zur Berufsmatur sollten Themen der Digitalisierung (z.B. Informatik und Medien) gehören. Medienbildung sollte am Gymnasium erweitert werden.
- Auch im Bereich Weiterbildung stellt sich die Frage nach einem individuellen elektronischen Bildungsportfolio. Zu klären sind hier Fragen wie: Soll es eine solche digitale Form von Zeugnissen geben? Was soll noch erhoben werden? Wie soll man diese Daten nutzen? Wer hat dabei welche Rechte? Diese Fragen könnten im Zusammenhang mit einer digitalen Identität geklärt werden. Hier soll aber Datensparsamkeit und informationelle Selbstbestimmung im Vordergrund stehen.
- Bei den Lehrmitteln sollen Anwendungen entwickelt werden, welche auf die einzelnen Schulfächer oder den zu vermittelnden Stoff zugeschnitten sind.

Empfehlung:

45. Bund und Kantone schaffen in enger Zusammenarbeit mit allen betroffenen Kreisen der Gesellschaft und Wirtschaft die strukturellen Voraussetzungen, um die Weiterbildung für Berufsleute aller Bereiche zwecks Bewältigung der digitalen Transformation zu erleichtern.

10.3.4 Kultur als Mittel für die digitale Aufklärung

Die Kultur eignet sich speziell als Kommunikationsmittel zur kritischen Reflexion. Darum soll die Kulturförderung stärker darauf ausgerichtet werden, dass sich Kulturschaffende aller Gattungen verstärkt kritisch-reflexiv mit dem digitalen Wandel auseinandersetzen.

Folgende Anregungen können dabei Beachtung finden:

- Kunst könnte die Begeisterung für das digitale Zeitalter wecken: interaktive, digitale Kunst, Computerspiele, Kurzfilme oder Kinofilme, usw. Das könnte in Museen oder an Festivals stattfinden. Kunst könnte auch beitragen, dass die Bevölkerung für Themen wie „Digitalisierung“ oder KI angemessen sensibilisiert wird, einen spielerischen Umgang damit findet und diese Themen kritisch reflektiert. Auch Krimis und TV-Serien eignen sich als Instrumente digitaler Aufklärung.

[18] Ein Beispiel ist der „Leitfaden zur Umsetzung der Basis-Absicherung nach IT-Grundschutz: In 3 Schritten zur Informationssicherheit“ des deutschen Bundesamtes für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3 [Stand Mai 2018]

- Man könnte digitales Kunstschaffen fördern, indem man z.B. einen Swiss Digital Art Prize schafft. Es könnten auch vermehrt Kunststipendien für solche Arbeiten gesprochen werden.
- Räume, wo man einen schöpferischen oder kreativen Umgang mit Digitalisierung ausprobieren kann, sollen gefördert werden. Dazu gehören Creative Spaces wie z.B. sog. Makerspaces, aber auch Bibliotheken, wo soziokulturelle Animation stattfindet. Zu empfehlen sind auch öffentliche Hackathons und das erweiterte Konzept von City Challenges bzw. Städteolympiaden (s. Ziff. 11). Eine „A Nation of Makers[19]“ Initiative würde „normalen“ Bürgerinnen und Bürgern sowie Jugendlichen helfen, innovative Ideen zu entwickeln und auszuprobieren. Die Open Innovation Initiative (die Öffnung des Innovationsprozesses von Organisationen für externes und internes Wissen zur Vergrösserung des Innovationspotenzials) oder die Idee von Living Labs (wo potenzielle Nutzer möglichst früh in den Entwicklungsprozess von neuen mobilen Anwendungen und Produkten wie z.B. Apps eingebunden werden) sind weitere Beispiele. Zu erwähnen ist ebenfalls die digitale Neuauflage von Gemeindezentren (Fablabs[20)]. Etwas Ähnliches gibt es in Amsterdam mit „De Waag“[21] oder in Fribourg mit der Bluefactory[22]. Der Bund könnte in allen Städten vergleichbare Projekte fördern, die die Begeisterung für das Thema wecken.

Empfehlung:

46. Bund und Kantone setzen sich für eine Kulturförderung ein, die sich verstärkt mit dem digitalen Wandel auseinandersetzt, und schaffen öffentliche Räume für den kreativen Umgang mit digitalen Technologien.

[19] https://nationofmakers.us/about.html [Stand Juli 2018]; Nation of Makers ist eine nationale Non-Profit-Organisation, die Amerikas Anhänger der Maker-Bewegung durch den Aufbau von Gemeinschaften, Sharing von Ressourcen und juristischen Beistand unterstützt.

[20] Offene Entwicklungswerkstätten, wo Interessierte Zugang zu High-Tech Werkzeugen wie 3D Druckern, Lasercuttern, CNC Fräsen, Mikrocontrollern, CAD Software, aber auch zu Handwerkzeug und Holzbearbeitungsmaschinen und fast allen anderen Tools, die man zum Basteln und Erfinden braucht, finden.

[21] http://waag.org/en [Stand November 2017].

[22] http://www.bluefactory.ch/en [Stand November 2017].

11 Analysefeld Digitale Transformation und Ethik

11.1 Ist-Zustand und weitere Entwicklung

11.1.1 Einführende Bemerkungen

Ethik ist eine Grundlage für eine nachhaltige Gesellschaft. Seit Jahrtausenden dient Moral als Verhaltensrahmen dazu, ein friedliches und erfolgreiches Zusammenleben im jeweiligen kulturellen und geschichtlichen Kontext zu fördern. Zwar lassen sich manche gesellschaftlichen Konflikte auf fundamentale Differenzen in Wertfragen zurückführen, die nicht einfach zu lösen sind. Dennoch haben sich im Laufe der Geschichte ethische Normen als Basis für das Zusammenleben in modernen, pluralistischen Gesellschaften erwiesen. Beispielsweise dienen die Menschenrechte dazu, ein selbstbestimmtes und selbstverantwortliches Leben zu ermöglichen und das Individuum vor Übergriffen des Staates, von Unternehmen und anderen Personen zu schützen. Grundfreiheiten wie die Meinungs-, Glaubens- und Informationsfreiheit sollen die Selbstentfaltung im ökonomischen und gesellschaftlichen Interesse fördern, soweit sie die Selbstentfaltung anderer nicht unbotmässig beschränken. Die Privatsphäre garantiert Erholungs- und Entfaltungsräume, die ein Experimentieren mit neuen Ideen und Lebensformen erlauben und dabei das Individuum in seiner Entfaltung und vor externen Eingriffen schützen.

Obgleich sich das hier geschilderte Verständnis moralischer Grundwerte vorab im westlichen Kulturraum entfaltete und sich Gesellschaften darin unterscheiden, wie genau sie ethische Werte wie Freiheit, Gleichheit oder Gerechtigkeit verstehen, bilden die grundlegenden Menschenrechte einen international breit abgestützten ethischen Orientierungsrahmen. Natürlich können Wertkonflikte vorkommen; beispielsweise, wenn Freiheitsrechte von Individuen mit Solidaritätsansprüchen von Gruppen kollidieren. Aufgabe der Ethik ist es dann, die Argumente für den jeweiligen Standpunkt kritisch zu prüfen und die entsprechenden Einschätzungen in den gesellschaftlichen Diskurs einzubringen. Eine Herausforderung in modernen, pluralistischen Gesellschaften besteht darin, dass ein Konsens über das „richtige" Verständnis von ethischen Werten nicht vorausgesetzt werden kann, sondern für den jeweiligen Konflikt ausgehandelt werden muss. Wie weit sollen beispielsweise solidarische Verpflichtungen in einer Krankenversicherung gehen, wenn Einzelne bewusst Gesundheitsrisiken eingehen? Solche ethischen Fragen bilden den Kern vieler gesellschaftlicher Debatten.

Verändern sich Gesellschaften aufgrund sozialer Entwicklungen oder technologischer Innovationen, hat dies einen Einfluss auf die in einer Gesellschaft herrschende Moral. So kann sich das Verständnis bestimmter Werte verändern, oder deren Bedeutung nimmt in gewissen Fragestellungen zu oder ab. Nimmt man beispielsweise die Demokratie als ethischen Grundwert der Organisation einer Gesellschaft, so lassen sich zwar deren Wurzeln auf die Stadtstaaten im antiken Griechenland zurückführen, doch das Verständnis des Werts Demokratie hat sich seitdem deutlich gewandelt – etwa indem der Einbezug von Frauen oder Menschen mit wenig finanziellen Mitteln im demokratischen Entscheidungsprozess heute selbstverständlich ist. Auch wenn es unterschiedliche Formen von Demokratie gibt – zum Beispiel direkte oder repräsentative Demokratie – betrachten wir diese Staatsform als schützenswert und zukunftsfähig, weil sie die Einbindung sowie Ausbalancierung unterschiedlicher Standpunkte und Interessen ermöglicht. Nach heutigem Wissen schafft dies die besten Voraussetzungen für Frieden, Wohlstand und Stabilität. Wichtige Charakteristika und Funktionsprinzi-

pien von Demokratien sind u.a. Freiheit (inkl. Presse- und Meinungsfreiheit), Selbstbestimmung, -entfaltung und -verantwortung, Pluralismus, Gewaltenteilung, Machtteilung, Checks and Balances, Minderheitenschutz, Mitbestimmung, Transparenz, Fairness, Gerechtigkeit, Legitimität und Schutz der Privatsphäre. Insgesamt kann gesagt werden, dass viele dieser Werte als Reaktion auf gravierende Ereignisse wie Kriege, totalitäre politische Systeme oder Genozide in der Verfassung verankert wurden. Sie bilden damit das Fundament für unsere moderne Gesellschaftsordnung.

11.1.2 Von der Digitalisierung betroffene Grundwerte

Welche ethischen Werte spielen nun für den Kontext der Digitalisierung eine besondere Rolle? Ohne Anspruch auf Vollständigkeit sind dabei insbesondere folgende Werte zu nennen:

- **Menschenwürde und Privatsphäre:** Die Allgemeine Erklärung der Menschenrechte von 1948 (UN-Menschenrechtscharta) beginnt mit dem Satz „Alle Menschen sind frei und gleich an Würde und Rechten geboren". Obgleich die rechtliche Konkretisierung von Menschenwürde nicht einfach ist, kommt damit ein unveräusserlicher Wert und die Verpflichtung zum Schutz des Menschen zum Ausdruck. Menschenwürde bedeutet unter anderem, dass Menschen nicht rein als Mittel zum Zweck verwendet oder gewissermassen zu einer „Ware" werden dürfen. Im Kontext der Digitalisierung sind die informationelle Selbstbestimmung und der Schutz der Privatsphäre wichtiger Ausdruck der Menschenwürde. Dies verlangt insbesondere, dass niemand willkürlichen Eingriffen auf sein Privatleben, seine Familie, sein Heim und seinen Briefwechsel oder Angriffen auf seine Ehre und seinen Beruf ausgesetzt werden darf. Dies ist auch explizit Gegenstand der UN Menschenrechtscharta, für deren Umsetzung die jeweiligen Staaten verantwortlich sind. Ziel dieser Bestimmung ist es, Lebensbereiche der Individuen zu schützen, in denen diese sich frei bewegen, entwickeln und verhalten können. Privatsphäre beinhaltet damit nicht nur einen Schutz vor Entblössung, sondern auch ein Recht, in Ruhe gelassen zu werden, also auch das Recht, sich von personalisierten manipulativen Einflüssen abzuschirmen und vor ihnen im privaten Umfeld geschützt zu werden. Zudem ist mit Privatsphäre auch das Recht verbunden, sich abzugrenzen, nicht ständig zur Verfügung zu stehen oder offline zu sein.
- **Gleichheit und Diskriminierungsverbot:** Gleichheit ist eine Grundnorm der Gesellschaft, die sich im Grundsatz der Gleichheit vor dem Gesetz widerspiegelt. Gemeint ist damit nicht, dass es grundsätzlich ethisch falsch sei, Personen ungleich zu behandeln, beispielsweise indem sie aufgrund unterschiedlicher Leistungen unterschiedliche Löhne erhalten. Ethisch problematisch wird es aber dann, wenn dabei Kriterien wie die Hautfarbe, das Geschlecht oder die Religion eine Rolle spielen, welche im Hinblick auf den Zugang zu bestimmten Gütern, Chancen und Positionen nicht relevant sind. Dann spricht man von Diskriminierung, also von einer Ungleichbehandlung von Personen, die sachlich nicht gerechtfertigt ist.
- **Autonomie und Selbstbestimmung:** Der Grundsatz der Autonomie gibt Menschen Rechte (und Pflichten) hinsichtlich der Gestaltung und der Kontrolle des eigenen Lebens. Die Bedeutung von Autonomie und Selbstbestimmung schlägt sich auch im Prinzip der informierten Zustimmung (informed Consent) nieder. Im digitalen Kontext spricht man von der informationellen Selbstbestimmung. Gemeint ist hier das Recht des Einzelnen, selbst über das Erheben, Speichern, Verwenden und Weitergeben persönlicher Daten bestimmen zu können.

- **Transparenz:** Damit Menschen ihre Autonomie und Mitwirkungsrechte wahrnehmen können, brauchen sie Wissen über die sie betreffenden Angelegenheiten. Der politische Diskurs braucht eine offene und relevante Kommunikation bezüglich der zur Debatte stehenden Entscheidungen. Nur so können die Akteure sich eine gut informierte Meinung bilden und freie Entscheidungen treffen – Transparenz ist somit auch eine Voraussetzung für informierte Zustimmung zur Verwendung persönlicher Daten.
- **Solidarität:** Solidarität bezeichnet die Verbundenheit der Einzelpersonen in einer Gemeinschaft. Einzelpersonen werden also in Bezug auf bestimmte Risiken und Gefahren, denen sie in ihren Aktivitäten und in ihrem Leben ausgesetzt sind, nicht allein gelassen. Die Gemeinschaft unterstützt sie bei der Bewältigung von Notsituationen wie Krankheiten und Unfällen sowie Armut. Dahinter steht die Einsicht, dass jeder auch ohne sein Verschulden krank oder arm werden kann und dass ohne Solidarität die Risikobereitschaft abnimmt – diese ist aber eine Voraussetzung für Innovation und Unternehmergeist, die von gesellschaftlichem Interesse sind
- **Sicherheit:** Eine zentrale Aufgabe des Gemeinwesens ist es, Leben und Eigentum zu schützen. Sicherheit als Grundwert meint damit nicht nur den unmittelbaren Schutz vor Raub, Verletzung oder gewaltsamem Tod, sondern auch die Gewährleistung von materiellen Voraussetzungen, damit die oben genannten Werte auch wirklich gelebt werden können; gemeint ist ebenso die Sicherung des Friedens, weil unter Konflikt- und Kriegsbedingungen Grundrechte ausser Kraft gesetzt werden können.

Diese Werte bilden wichtige, fundamentale Orientierungspunkte, auch wenn sie manchmal in Konflikt zueinanderstehen – etwa, wenn Freiheitsrechte mit Solidaritätspflichten kollidieren. Es ist Aufgabe von Politik und Gesellschaft, diese Werte in eine Balance zu bringen und darauf zu achten, dass Dilemmata zwischen Werten durch innovative Lösungen möglichst vermieden oder überwunden werden.

11.1.3 Konkrete ethische Probleme

Die momentan stattfindende Digitalisierung verändert die Gesellschaft tiefgreifend und hat damit auch einen Einfluss auf deren ethisches Fundament. Der Vergleich mit der im 18. Jahrhundert begonnenen Industrialisierung drängt sich auf, aber die Umwälzungen werden diesmal voraussichtlich noch schneller und umfassender sein. Die Herausforderung besteht darin, diesen historischen Transformationsprozess so zu gestalten, dass er friedlich und ohne gewaltsame Revolutionen und Kriege verläuft.

Ob Wissensverwaltung, Logistiknetze oder gar die Anbahnung menschlicher Beziehungen: Digitale Technologie durchdringt unsere Lebenspraxis inzwischen in fast allen Bereichen. Sie verändert Informationsflüsse und die Organisation vieler Prozesse. Immer mehr soziale Sphären werden von digitalen Systemen bevölkert, ausgestattet mit Sensoren, Effektoren und dazwischengeschalteter Informationsverarbeitung. Sie wirken als technische Mediatoren von Produktionsprozessen und menschlichen Beziehungen. Zudem transportieren Informatik und Computerwissenschaften – die Leitwissenschaften der Digitalisierung – eine ganz bestimmte Sicht auf die Welt: Sie wird verstanden als ein Konglomerat von Informationen und Informationsflüssen. Der Versuch der Beherrschung der Welt drückt sich darin aus, diese Informationsflüsse messen und beeinflussen zu wollen.

Praktisch geht damit die Gefahr einher, dass die Werkzeuge der Digitalisierung auch

unethischen Zwecken dienen können (dual Use). Nach Einschätzung vieler Expertinnen und Experten können sie gesellschaftliche Errungenschaften bedrohen. Beispiele von Nutzung digitaler Technologie, die potenziell unerwünschte Auswirkungen haben können, sind:

- **Digitalisierung der Arbeitswelt:** Auswirkungen der Digitalisierung auf die Arbeitswelt sind in jüngster Zeit stark diskutiert worden. Die beschleunigte Automatisierung durch KI und Robotik kann Arbeitsplätze und die ökonomische Teilhabe bedrohen, was die Gefahren sozialer Ungleichheit verstärkt. Käme es zu einem deutlichen Rückgang von Arbeitsmöglichkeiten, könnten ein Recht auf Arbeit und Einkommen sowie die Möglichkeit der Selbstverwirklichung durch Arbeit unterminiert werden. Dies wäre eine Entwicklung, welche letztlich auch die staatlich aktiv zu schützende Menschenwürde tangieren könnte. Zudem beruht ein wesentlicher Teil der Einkünfte des Staates auf der Besteuerung von Arbeitseinkommen – entsprechende Einbussen könnten daher das Gemeinwohl und die politische Stabilität gefährden. Natürlich ergeben sich durch den technologischen Wandel auch grosse wirtschaftliche und gesellschaftliche Chancen. Während der digitalen Transformation kann es jedoch zu disruptiven Entwicklungen kommen, die zur Gewährleistung von Sicherheit und Frieden politisch so weit wie möglich abzufedern wären. Es ist auch klar, dass die Digitalisierung der Arbeitswelt grosse Auswirkungen darauf hat, welche beruflichen Kompetenzen künftig nötig sind, um in der Wirtschaft zu bestehen. Entsprechend ist das Bildungswesen gefordert, was im Analysefeld „Digitale Aufklärung der Bevölkerung, Kompetenzaufbau, Mitgestaltung des Nutzers und Forschung" ausgeführt ist (s. Ziff.10).
- **Massenüberwachung:** Eine umfangreiche Überwachung, beispielsweise grosser Teile des Internet-Verkehrs, unterminiert die Privatsphäre der Bürgerinnen und Bürger und damit deren persönliche Freiheit, Selbstbestimmung und Selbstentfaltung. Dies kann indirekt zu Selbstzensur und zu einer Verminderung von politischer Meinungsvielfalt und gesellschaftlichem Engagement führen, was die Funktionsfähigkeit des demokratischen Gemeinwesens mindert. Das Ausmass der Massenüberwachung illustrieren die verschiedenen, bekannt gewordenen Überwachungsprogramme der NSA und CIA sowie das britische „Karma Police" Programm. Viele Staaten benutzen ausgefeilte Techniken zur gezielten Überwachung, Behinderung oder gar Bedrohung von Dissidenten.
- **Soziale Medien:** Die derzeitige Art der Nutzung sozialer Medien und der zunehmende Einsatz „sozialer Bots" unterstützen Phänomene wie „Shit Storms" und „Fake News". Sie sind weder Garant für qualitativ gute oder ausgewogene Information noch wirken „Filterblasen" und „Echokammern" der gesellschaftlichen Polarisation entgegen. Gleichzeitig werden die Instrumente zur Veränderung medialer Inhalte raffinierter, und es ist absehbar, dass es zunehmend schwierig wird zu erkennen, ob gewisse Inhalte, Bilder, Videos oder Tonaufnahmen echt oder gefälscht sind; dies eröffnet neue Möglichkeiten zur Beeinflussung von politischen Prozessen auch durch Drittstaaten, was die soziale Stabilität eines Landes gefährden kann. Überhastete Gegenreaktionen können zur Bildung von „Wahrheitsbehörden" (im Sinne des Romans „1984" von George Orwell) führen und damit ebenfalls demokratische Grundrechte wie die Presse- und Redefreiheit gefährden. Ein bewusster Umgang mit den Möglichkeiten sozialer Medien ist deshalb eine weitere zentrale Herausforderung für das Bildungswesen, was im Analysefeld „Digitale Aufklärung der Bevölkerung, Kompetenzaufbau, Mitgestaltung des Nutzers und Forschung" ausgeführt ist (S. Ziff. 10).

- **Big Nudging:** Unter „Big Nudging" versteht man den Versuch, mittels personalisierter Information eine Verhaltensbeeinflussung einer grossen Zahl von Menschen auch auf unbewusster Ebene zu erreichen, um damit z.B. politische Ziele zu verfolgen. Ein solches Big Nudging beinhaltet einen Wertekonflikt zwischen Wohlfahrt und Autonomie der Bürgerinnen und Bürger und ist insbesondere dann ethisch problematisch, wenn es intransparent und unausweichlich ist. Personalisierung z.B. in der Werbung gehört zum Geschäftsmodell zahlreicher Firmen, die Internet-Services (Suchmaschinen, soziale Netzwerke) anbieten und entsprechende Nutzerdaten sammeln. Das Tauschgeschäft „Gratisnutzung gegen personalisierte Werbung" ist zwar den meisten Nutzern solcher Plattformen bekannt, doch die jüngst bekannt gewordenen Beispiele (z.B. Facebook) zeigen die Problematik des Missbrauchs solcher Daten für Big Nudging im Rahmen möglicher Wahlmanipulationen, wie sie 2016 im Zusammenhang mit dem „Brexit“ und der US Präsidentschaftswahl thematisiert wurden. Die Effektivität solcher Manipulationen wird zwar kontrovers diskutiert. Unbestritten ist aber, dass ein intransparenter Missbrauch von Daten vorliegt, der auch die Privatsphäre der Nutzer verletzt. Die zunehmende Erfassung von Datenströmen (z.B. zu Stromverbrauch, Verkehr etc.) kann zudem zu einem undemokratischen Versuch staatlicher Verhaltenssteuerung führen, was freies und eigenverantwortliches Handeln einschränkt. Eine in Zukunft mögliche breite Anwendung von Big Nudging könnte das Selbstverständnis, wonach unsere Gesellschaft auf freier, selbstverantwortlicher Mitgestaltung beruhen soll, nachhaltig unterminieren.
- **Prädiktive Modellierung und Kontrolle:** Eng mit dem Thema Big Nudging verbunden ist die Nutzung digitaler Technologie zur Vorhersage und Kontrolle sozialer Prozesse. Die Einbeziehung eines Individuums in Entscheidungsprozesse, die für dieses von Belang sind, ist ein wesentliches Charakteristikum der Menschenwürde, welche als unveränderlicher Grundpfeiler von Demokratien angesehen wird. Der Respekt der Menschenwürde erfordert, dass menschliche Subjekte nicht wie Tiere, Objekte oder Daten behandelt werden. Im demokratischen Rechtsstaat werden Menschen daher aufgrund ihres tatsächlichen Verhaltens zur Rechenschaft gezogen – beispielsweise im Kontext des Strafrechts. Ihnen ist dabei ein Widerspruchsrecht zu gewähren. Moderne Datenverarbeitung könnte ein verantwortungsbewusstes Abwägen individueller Entscheidungsträger auf der Basis eines „ethischen Kompasses" durch automatisierte Vorhersagealgorithmen ersetzen. Prädiktive Modellierung könnte zu einem umfassend angewendeten Risikomanagement in vielen Bereichen der Gesellschaft führen. Beispielsweise könnten Algorithmen zur Vorhersage unerwünschten Verhaltens – wie das sogenannte „predictive Policing" – die Unschuldsvermutung im Rechtssystem untergraben, aber auch das Experimentieren mit neuen, innovativen Lösungen behindern. Der Wert der Selbstverantwortung würde dadurch stark beeinträchtigt, und in letzter Konsequenz würde dem Menschen die Freiheit genommen, für seine Taten Verantwortung zu übernehmen.
- **Citizen Score:** Ein konkreter Ausdruck von Verhaltenssteuerung ist das in China derzeit entwickelte Sozialkredit-System („Social Credit" oder „Citizen Score"). Mit diesem teilweise schon realisierten Konzept einer digitalen sozialen Kontrolle wird politisch oder wirtschaftlich erwünschtes Verhalten erzwungen, indem der persönliche Punktestand beispielsweise über den Zugang zu Arbeitsplätzen, Dienstleistungen oder Kreditkonditionen entscheidet. Dies zerstört den gesellschaftlichen Pluralismus und fördert Untertanenmentalität statt verantwortungsbewusst entscheidende Bürgerinnen und Bürger. Im Zusammenhang mit Res-

sourcenknappheiten kann der Citizen Score zu schwerwiegenden Benachteiligungen vieler Bürger und Bürgerinnen führen. Solche Methoden bedrohen die Grundvoraussetzungen eines menschenwürdigen Lebens.

- **Vollautomatisierte Entscheidungsalgorithmen**: Eine zunehmend datengestützte Beeinflussung des digitalen Zugangs zur Welt und eine verstärkte Nutzung automatisierter Entscheidungsalgorithmen können Fairness und Gerechtigkeit bedrohen. Ein allgemeines Problem ist, dass das „Trainieren“ solcher Algorithmen auf Daten aus der Vergangenheit beruht, was zu einer „Verfestigung“ von Vorurteilen und veralteten Lösungen führen kann. Beim autonomen Fahren und generell bei autonomen Entscheidungen künstlicher Intelligenzsysteme können sogar Entscheidungen über Leben und Tod auftreten. Dies führt zu ethischen Dilemmata, die heute zwar im Prinzip implizit auch vorhanden sind (in seltenen Fällen gibt es Unfälle, bei denen der Fahrer sich zwischen zwei schlechten Lösungen rasch entscheiden muss), die aber expliziert werden müssten, wenn Algorithmen sie in Zukunft lösen sollen. Die Explizierung solcher Dilemmata birgt das Risiko, dass man „Wertigkeiten" von Menschen gegeneinander aufrechnet. Unter Juristen und Ethikern herrscht aber die Auffassung vor, dass keine unterschiedliche Wertigkeit des Menschen (etwa auf der Basis von Alter, Bildung, Einkommen) zugrunde gelegt werden darf und von Gesetzes wegen alle Menschen gleich zu behandeln sind. Deshalb ist das Auftreten von Dilemmata, bei denen Menschen sterben können, durch geeignete technische, politische und gesellschaftliche Lösungen zu minimieren. Technische Systeme können einen Beitrag leisten, falls deren Anwendung die Zahl dilemmatischer Situationen vermindert und z.B. eine allgemeine Programmierung zur Minimierung der Zahl der Personenschäden enthalten. Dabei sind zur Vermeidung unterschiedlicher Wertigkeit auch zufallsbasierte Lösungen in Betracht zu ziehen. Wenn jedoch der Einsatz solcher Systeme dazu führt, dass die Zahl der zu explizierenden Dilemmata (d.h. Dilemmata, für die der Algorithmus eine Lösung bereithalten muss) zunimmt, ist ihr Einsatz nicht vertretbar. Besonders problematisch sind in diesem Zusammenhang Entwicklung und Einsatz autonomer Waffensysteme. Daher ist bei der Implementierung und Anwendung automatisierter Entscheidungsalgorithmen Transparenz über die Grundlage der Entscheidungsfindung, Nachvollziehbarkeit und Verantwortung („meaningful human Control“) gefordert. Dies ist auch dann wichtig, wenn die Entscheidungsalgorithmen nicht in potenziell dilemmatischen Situationen eingesetzt werden. So finden solche Systeme zunehmend Einsatz bei der kommunikativen Interaktion mit Menschen. Wenn aus dem Kontext nicht ersichtlich ist, dass ein Mensch mit einer Maschine kommuniziert, ist dies eine Form der Täuschung mit möglicherweise nachteiligen Folgen für den menschlichen Gesprächspartner (z.B. könnten die Reaktionen des Menschen zwecks Optimierung der Sprachfunktion des Algorithmus aufgezeichnet werden). In solchen Situationen sollten demnach die menschlichen Gesprächspartner vorgängig informiert werden, wenn sie mit einem Sprachsystem interagieren.

- **Cyberrisiken:** Die Durchdringung von immer mehr Lebensbereichen durch digitale Technologie (z.B. „Internet of Things") macht kritische Infrastrukturen anfälliger für Manipulation, Diebstahl, Sabotage oder Zerstörung, was Sicherheit und Frieden gefährdet. Eine zu starke Betonung von Cybersecurity als Reaktion auf Cyberrisiken kann zudem mit Grundwerten in Konflikt geraten und diese beeinträchtigen. Problematisch ist in diesem Zusammenhang die Tatsache, dass Geheimdienste Schwachstellen in Software (so genannte „Zero Day Exploits") horten und nicht öffentlich bekannt machen, was Abwehrmassnahmen unterminiert

(ein Beispiel sind die „WannaCry" Ransomware Attacken vom Mai 2017). Generell sind durch Cyberrisiken sowohl die individuelle Souveränität als auch die Souveränität von Unternehmen und Staaten zunehmend gefährdet.

11.1.4 Grundlegende ethische Herausforderungen

Diese Beispiele von ethisch fragwürdigen Aspekten digitaler Technologien verweisen auf einige grundlegende Probleme, die mit der Digitalisierung einhergehen und die bereits im Kapitel „digitale Aufklärung“ angesprochen wurden.

So ermöglicht erstens die Digitalisierung eine Quantifizierung zahlreicher Lebensbereiche, indem bislang implizit vorhandene Informationen explizit gemacht werden – die Vermessung der Gesellschaft erreicht daher ungeahnte Ausmasse. Menschen erhalten damit neue Möglichkeiten für den gegenseitigen Vergleich. Jene, die sich dieser Vermessung entziehen wollen, wirken zunehmend verdächtig oder geraten unter Druck, ihre Daten ebenfalls preiszugeben. Zudem reduzieren sich damit die gesellschaftliche Stellung des Menschen und sein Leben zunehmend auf das Messbare. Dies führt zu einer vereinfachten, manchmal sogar eindimensionalen Repräsentation des Menschen oder der Wirklichkeit (egal, ob es sich um einen Citizen Score, Geld, oder eine andere Grösse handelt). Ein solcher Ansatz führt früher oder später dazu, dass Zahlen zu viel Bedeutung oder Macht erhalten, wodurch die Menschlichkeit unter die Räder kommt.

Fraglich ist hier auch, ob die Idee eines „Dateneigentums" ein geeignetes Instrument ist, um diesen Quantifizierungsprozess in ethischer Hinsicht zu steuern. Zum einen würde damit ein Anreiz geschaffen, noch mehr Daten zu schaffen. Zum anderen ist gar nicht klar, inwieweit „persönliche Daten" auch wirklich nur der betreffenden Person gehören. Viele persönliche Daten betreffen Interaktionen mit Dritten: Ein Foto kann z.B. nicht nur die Person selbst, sondern auch Familienmitglieder zeigen; Daten über Vernetzungen auf sozialen Netzwerken mit Dritten sagen auch etwas über diese Personen aus. Solche persönlichen Daten sind so gesehen in vielen Fällen nicht ausschliesslich „Eigentum" einer einzigen Person – ähnlich, wie die genetischen Daten einer Person auch Aussagen über deren Verwandte erlauben. Entsprechend besteht die Herausforderung der Quantifizierung darin, ein genügendes Ausmass kritischer Reflexion und Möglichkeiten informationeller Selbstbestimmung zu fördern, damit Chancen und Risiken der durch die Digitalisierung vorangetriebenen Messbarkeit realistisch eingeschätzt werden können und gestaltbar werden. Dieser Punkt wird im Analysefeld Digitale Aufklärung der Bevölkerung, Kompetenzaufbau, Mitgestaltung des Nutzers und Forschung weiter ausgeführt.

Zweitens wird durch die Digitalisierung die Abhängigkeit des Menschen von Technologie auf eine neue Stufe gehoben, weil Maschinen zunehmend autonom agieren und dabei Entscheidungen fällen, die Menschen betreffen. Dies behindert menschliche Einflussmöglichkeiten und birgt die Gefahr, dass Menschen „maschinenkompatibel" gemacht werden – etwa zum Zweck der automatisierten Erfassung der Identität einer Person. Zahlreiche digitalisierte Prozesse verlangen eine Authentifizierung von Personen, z.B. bei Finanztransaktionen oder Zugangskontrollen. Dies ist unproblematisch, solange diese Authentifizierung für die jeweils betroffene Person bewusst und freiwillig geschieht; was aber bei Massnahmen wie z.B. dem „Chippen" einer Person (dem Implantieren eines Mikrochips zur automatisierten Identitätserfassung) nicht mehr der Fall wäre. Auch dieser Punkt wird im Analysefeld „Digitale Aufklärung der Bevölkerung, Kompetenzaufbau, Mitgestaltung des Nutzers und Forschung“ ausgeführt (s. Ziff. 10).

Drittens gibt es eine Tendenz bei der Nutzung digitaler Technologie, wonach Systeme, Prozesse und Abläufe immer mehr standardisiert werden, weil sich gewisse Lösungen

gegenüber anderen durchsetzen. Dies könnte zu einer übermässigen „Vereinheitlichung" auf globaler Ebene führen. Dies würde aber die Resilienz (Krisenfestigkeit) der menschlichen Gesellschaft unterminieren, denn diese braucht Diversität und experimentelle Freiräume, um langfristig das Überleben zu sichern. Entsprechend besteht hier die Herausforderung der Erhaltung menschlicher Kontrolle und Entscheidungsfähigkeit, damit Menschen nicht zu „funktionellen Einheiten" in einem komplexen soziotechnischen System degradiert werden, was mit Menschenwürde nicht vereinbar wäre. Dies kann weitreichende Auswirkungen auf die Entfaltungsmöglichkeiten des Menschen haben, welche die Grundlage der Innovationskraft unserer Gesellschaft sind. Man muss sich vor Augen führen, dass alle grossen gesellschaftlichen Innovationen zunächst gegen die Prinzipien des bestehenden Systems verstossen. Ohne die Möglichkeit von wohl überlegten Verstössen (sog. „disruptiven Innovationen“) wird die gesellschaftliche Fortentwicklung, wie sie gerade angesichts der zahlreichen zu lösenden globalen Probleme erforderlich ist, stark behindert. Damit ist zu befürchten, dass die Gesellschaft ihre Herausforderungen nicht rechtzeitig bewältigen und folglich in schwere Krisen geraten wird.

Ein vierter grundsätzlicher Punkt ist, inwieweit die Digitalisierung das ethische Fundament einer Gesellschaft bedroht. Ein wichtiger Ansatz zur Beantwortung dieser Fragen beruht auf dem Konzept der kontextuellen Integrität: Die Lebenswelt des Menschen ist in verschiedene Bereiche gegliedert, die für das Individuum verschiedene Orientierungsmassstäbe liefern. Menschen erwarten, in einem familiären Kontext anders behandelt zu werden als gegenüber einer staatlichen Organisation. Sie akzeptieren in einem ökonomischen Kontext Formen der Ungleichbehandlung, die man im Gesundheits-, Rechts- oder Bildungswesen nicht akzeptieren würde. Die Interpretation moralischer Grundwerte wie z.B. Gerechtigkeit, Autonomie und die damit verbundenen Regeln (im Fall von Gerechtigkeit Allokationsregeln wie „jedem das Gleiche“, „jedem das, was er verdient“ oder „jedem das, was er braucht“) unterscheiden sich je nach sozialer Sphäre. Entsprechend unterscheiden sich auch die Informationen, die in diesen verschiedenen Sphären erzeugt und von den Individuen dosiert preisgegeben werden – man spricht von der kontextuellen Integrität der Information.

Wenn eine Person beispielsweise im Kontext des Gesundheitswesens persönliche Daten der medizinischen Forschung zur Verfügung stellt, ist der Wunsch, Dritten zu helfen, oft das entscheidende Motiv. Werden diese Informationen nun aber verwendet, um etwa Versicherungsangebote masszuschneidern oder Profite zu maximieren, so entspricht dies nicht mehr der ursprünglichen Absicht – die kontextuelle Integrität der Information wird verletzt und untergräbt damit die Hilfsbereitschaft.

Techniken der Digitalisierung wie beispielsweise Big Data Analytics, die danach streben, möglichst viele verschiedene Informationen über Individuen unstrukturiert zu erfassen, tragen das inhärente Risiko in sich, diese kontextuelle Integrität zu verletzen. Da Daten zunehmend von Daten-Brokern gehandelt werden und in komplexe statistische Modelle von Personengruppen einfliessen, ist eine solche Verletzung der kontextuellen Integrität selbst für die kommerziellen Nutzer der Daten schwer oder nicht erkennbar. Wie gross das ethische Problem einer Verletzung der kontextuellen Integrität ist, ist zwar nicht einfach zu bewerten, da die Grenzen der verschiedenen sozialen Sphären und der darin herrschenden moralischen Normen nicht unveränderlich sind. Die Gewichtung von Werten kann sich beispielsweise verschieben, wenn Individuen bereit sind, mehr Informationen aus ihrem privaten Bereich im Gegenzug für individuelle oder kollektive Vorteile preiszugeben und dies ebenso von ihren Mitmenschen erwarten. In diesem Fall würde sich die gängige Vorstellung von Privatsphäre ändern. Allerdings bleibt zu bedenken, dass die Ordnung der Welt in verschiedene soziale Sphären mit verschiedenen Wertmassstäben zentral ist. Zum Beispiel würden viele

Menschen entrüstet reagieren, wenn private Informationen aus ihrem Freundeskreis zur Bildung individualisierter Preise oder Versicherungsangebote genutzt würden. Aus dieser Perspektive wird der allumfassende Charakter der Digitalisierung als einer Technologie, welche die Grenzen der sozialen Sphären aufweicht, als ethisches Grundproblem verstanden.

11.2 Möglichkeiten und Grenzen (Soll-Zustand)

11.2.1 Aktuelle Initiativen

Angesichts der Vielfalt an ethischen Herausforderungen der Digitalisierung gibt es aus der Sicht der Ethik nicht immer einfache Lösungen. Ein Mittel für den Umgang mit unbeabsichtigten und oftmals unerwarteten Nebenwirkungen sowie Missbrauchsmöglichkeiten digitaler Technologien sind die Technikfolgenabschätzung und Regulierung. Im Falle der digitalen Revolution laufen die innovativen Entwicklungen aber so schnell ab, dass diese Instrumente oftmals Mühe haben, mit dem rasanten Tempo Schritt zu halten. Sie stossen damit im Fall der Digitalisierung an ihre Grenzen.

Im Bereich der Regulierung gibt es einige Initiativen, um den Risiken der Digitalisierung zu begegnen. Auf EU-Ebene wurde eine Initiative zur Etablierung digitaler Grundrechte in die Wege geleitet. Einen ähnlichen Vorstoss hatte auch der ehemalige deutsche Justizminister Heiko Maas unternommen. Diese Initiativen gehen über die DSGVO hinaus, da sie vor allem die Durchsetzung der Grundrechte im digitalen Raum zum Ziel haben. Schon zuvor hatte die Regierung der USA, angesichts zahlreicher kritischer Stimmen aus Wissenschaft und Wirtschaft, die vor superintelligenten Systemen und autonomen Waffen gewarnt hatten, eine Serie von Workshops zur Zukunft der KI veranstaltet. Daraus gingen die IEEE Standards für „Ethically Aligned Design“ hervor.[23] Erstmalig haben sich auch die fünf IT-Giganten Alphabet (Google), Amazon, Facebook, IBM und Microsoft in einer gemeinsamen Initiative zusammengeschlossen, um schnellstmöglich zu einem ethischen Design von künstlichen Intelligenzsystemen zu gelangen. Das Ziel ist, „moral“ and „accountable“ KI zu entwickeln.

Aufgabe der Ethik ist aber nicht nur, vor möglichen Fehlentwicklungen zu warnen. Sie muss auch ein kritisches Auge auf übertriebene Hoffnungen und Ängste werfen, die mit der Digitalisierung im öffentlichen Diskurs verbunden werden. Eine verzerrte Problemwahrnehmung kann zu falschen Schlüssen und zu Lösungen führen, die ethisch ebenfalls problematisch sein können. Beispielsweise wurde im Zuge der jüngsten politischen Entwicklung im öffentlichen Diskurs die These vertreten, soziale Medien hätten entscheidend zur politischen Polarisierung beigetragen – die Evidenzlage zu dieser Frage ist aber alles andere als klar, und es existieren dazu widersprüchliche Befunde. Würden aufgrund solcher Thesen beispielsweise umfassende Zensurmassnahmen ergriffen, um das Problem von Fake News zu entschärfen, wäre das jedoch eine Massnahme, welche demokratische Grundwerte gefährden würde. Eine sorgfältige Abwägung der Problemlage unter Berücksichtigung von alternativen, dezentralen Lösungsansätzen (Stichwort: „Mechanism Design“) ist deshalb unbedingt erforderlich. Denkbar ist beispielsweise die verstärkte Nutzung von Reputations-, Qualifikations- und Moderationsmechanismen.

[23] Ethically Aligned Design, http://standards.ieee.org/news/2016/ethically_aligned_design.html [Stand Juni 2018].

11.2.2 Ethik als Motor für Innovation

Im Übrigen hat Ethik nicht nur eine „Wachhund-Funktion", sondern sie soll auch darüber aufklären, wie sie innovative Lösungen fördern kann. Es ist also ihre Aufgabe zu informieren, wie die Entwicklung besserer digitaler Technologien ermöglicht werden kann. Dies verlangt insbesondere die Schaffung eines Bewusstseins bei den Technologie-Entwicklern, inwieweit deren Anwendungen Grundwerte beeinträchtigen oder stärken können. Ein hierfür wichtiges Konzept ist der sogenannte „value-sensitive Design" Ansatz (auch „Ethically Aligned Design“ genannt). Ausgangslage hier ist die Beobachtung, dass technische Instrumente und Werkzeuge Werte implizieren, exemplifizieren oder es sogar verunmöglichen, bestimmten Werten Folge zu leisten. Dies gilt im besonderen Masse für informationstechnische Systeme, welche meist in komplexen, von Menschen geschaffenen Zusammenhängen zum Einsatz kommen: z.B. als Kommunikationshilfen (Handy, Skype etc.), als Planungsinstrumente (vom simplen Terminfinder Doodle bis zu komplexen Werkzeugen für die Konstruktion von Flugzeugen), für die Ideenentwicklung (kollektives Schreiben an Dokumenten etc.), für die Steuerung von technischen Systemen. In vielen solchen Systemen finden sich Default-Optionen, die schwer oder teilweise gar nicht veränderbar sind und die Wahrnehmung von Werten beeinflussen. Value-sensitive Design bedeutet dann zweierlei: Erstens eine grundsätzlich proaktive Haltung der Architekten von Informationssystemen gegenüber der Erkenntnis, dass ihre Erzeugnisse wichtige Werte wie Autonomie, Eigentum, Fairness, Freiheit, Identität, informierte Zustimmung, Privatheit, Vertrauen, Wohlfahrt oder Menschenwürde beeinflussen. Zweitens eine Systematik, diese Einflüsse so zu gestalten, dass sie mit den Grundwerten und kulturellen Werten kompatibel sind. Nötig sind hierbei:

- begriffliche Arbeit (Welche Werte sind von einer bestimmten Technologie betroffen? Wie differenziert sich dieser Wert, z.B. Vertrauen? Wer ist vom jeweiligen Wert direkt oder indirekt betroffen?);
- empirische Untersuchungen (Merken Anwender, dass die Nutzung bestimmter Technologien einen Trade-off von Werten – z.B. bequeme Nutzung vs. Privatheit – beinhaltet? Welche Unterschiede gibt es zwischen den Ansichten über bestimmte Handlungen und den tatsächlich durchgeführten Handlungen bei der Nutzung von Technologie?); und
- technische Analysen (durch welche technischen Eigenschaften drückt sich ein Wert in der Technologie aus? Wie kann ein gewünschter Wert – z.B. Kollaboration – durch das jeweilige Design der Technologie gefördert werden?). Wie kann verhindert werden, dass ein Verständnis von Werten (wie Privacy) in der Technologie eingebaut wird, das nicht dem Verständnis des Nutzers dieser Technologie entspricht?

Schliesslich ist es eine Aufgabe der Ethik darauf hinzuweisen, dass die Digitalisierung auch eine positive Rolle bei der Bewältigung künftiger Herausforderungen wie Klimawandel oder Ressourcenverknappung spielen kann. Beispielsweise[24] wurden zur schnellen Entwicklung von energie-, umwelt- und ressourcenschonenden Lösungen und ihrer Verbreitung Städteolympiaden vorgeschlagen. Darüber hinaus können durch Kombination des Internets der Dinge mit Blockchain-Technologie neue Marktkräfte angetrieben werden, die zu einer ressourcenschonenden, effizienten und konkurrenzfähigen Kreislaufwirtschaft und zu einer wirtschaftlichen Entwicklung führen, die mit den gesellschaftlichen Grundwerten konform ist und Externalitäten (also Auswirkungen auf

[24] http://futurict.blogspot.de/2017/06/propositions-on-perspective-global.html [Stand 25. Juni 2017].

Mensch und Umwelt) berücksichtigt. Der entsprechende Ansatz ist unter den Stichworten „sozio-ökologisches Finanzsystem“ bzw. „Finanzsystem 4.0“ bekannt geworden. Daneben wird häufig die Organisation der digitalen Wirtschaft als partizipatives und weitgehend offenes Innovations-Ökosystem empfohlen, damit kombinatorische Innovation möglich wird. In diesem Zusammenhang spielen einerseits Prinzipien wie Open Source, Open Access, Open Data, Open Innovation eine wichtige Rolle, andererseits Prinzipien wie Ko-Kreation, Ko-Evolution, kollektive Intelligenz, Selbstorganisation und subsidiär organisierte Governance. Zur Beschleunigung der Innovation wurde ausserdem der „demokratische Kapitalismus“ vorgeschlagen – eine Art „Crowdfunding für alle“, finanziert durch den Staat oder einen neuen Gelderzeugungsmechanismus. Ausserdem wurden neue Anreizsysteme und Wege gefunden, wie man kollektive Intelligenz erhöhen und damit Demokratie und Märkte wesentlich verbessern kann. Diese sind unter dem Stichwort „digitale Demokratie“ oder „digitales Upgrade für die Demokratie“ bekannt geworden. Schliesslich können auch konkrete Tools zur digitalen Befähigung generiert werden. So wurde beispielsweise kürzlich ein digitaler Datenassistent (basierend auf KI-Technologie) vorgeschlagen, der es den Bürgerinnen und Bürgern auf einfache Art und Weise ermöglichen soll, die Verwendung ihrer persönlichen Daten einzusehen, zu verstehen und zu beeinflussen.

11.3 Erkenntnisse

Die in diesem Kapitel ausgeführten ethischen Fragen und Lösungsmöglichkeiten lassen sich – im Unterschied zu den anderen Analysefeldern – in der Regel nicht in einfache Lösungen überführen, die ein Problem für immer „abhaken“. Viele der angesprochenen Probleme sind komplex und benötigen ein ganzes Bündel von Massnahmen, die nicht alle direkt die Ethik betreffen. Zudem haben viele der sonst in diesem Bericht vorgeschlagenen Massnahmen natürlich Bezüge zu ethischen Grundwerten, indem sie etwa der informationellen Selbstbestimmung und dem Schutz der Privatsphäre dienen. Aus diesem Grund formulieren wir hier an dieser Stelle nur zwei generelle Massnahmen:

1) **Ethik in der Aus- und Weiterbildung:** Fachleute aller Berufsgruppen, welche massgeblich die digitale Transformation prägen, sollten im Verlauf ihrer beruflichen Aus- und Weiterbildung regelmässig und konkret mit Ethik konfrontiert werden. Dieser Einbezug der Ethik sollte konstruktiv sein, d.h. es soll nicht darum gehen, Ethik als eine Form der „Überwachung und Kontrolle" zu vermitteln. Vielmehr soll verdeutlicht werden – z.B. durch Ansätze wie Design for Values oder value-sensitive Design –, wie ethisches Denken konstruktiv zu digitalen Lösungen beitragen kann. Dies betrifft nicht nur Ingenieure und Informatiker, sondern alle Berufsgruppen (z.B. Medienfachleute, Manager etc.), welche massgeblich zur digitalen Transformation der Gesellschaft beitragen. Zur Förderung einer Führungsrolle der Schweiz in diesem Gebiet sollte auch die Forschung zu den Themen „responsible Innovation“ und „Design for Values“ intensiviert werden.

Anregungen zur Konkretisierung dieser Massnahmen sind:

- An den Schweizer Hochschulen soll die **Forschung zu ethischen Fragen des digitalen Wandels intensiviert** werden. Dies beinhaltet die Einrichtung von neuen Professuren und Forschungszentren beispielsweise zum Thema „value-sensitive Design". Dabei ist insbesondere zu beachten, dass diese Professuren und Forschungszentren eine starke interdisziplinäre Ausrichtung haben und eng mit technischen und sozialwissenschaftlichen Forschungsgruppen kooperieren.

- Die **Forschung zu sozialwissenschaftlichen und technischen Themen** mit direkten Auswirkungen auf die oben genannten ethischen Probleme ist zu fördern. Zu nennen sind insbesondere Forschungen zu den Fragen, inwieweit digitale Manipulation tatsächlich reale Auswirkungen hat, wie die Transparenz und Prüfbarkeit von KI-Systemen mit Entscheidungsfunktionen verbessert werden kann, mit welchen Massnahmen „Filterblasen" bekämpft werden können oder in welcher Form ein „Dateneigentum" überhaupt auf sinnvolle Weise realisiert werden kann.
- Analog zum Ausbau der Forschungskapazität in den genannten Bereichen ist insbesondere in der **Ausbildung von technischen Fachspezialistinnen und -spezialisten** sicherzustellen, dass ethische Fragen genügend Gewicht erhalten. Zu nennen ist hier insbesondere der Bereich der Cybersecurity, wo beispielsweise das Bewusstsein möglicher Wertkonflikte geschärft werden muss (z.B. Informationssicherheit vs. Datenzugang im Gesundheitswesen) und best Practices für den Umgang mit solchen Wertkonflikten entwickelt werden sollten.

2) **Schutz der Grundwerte:** Konkrete Massnahmen, die sich als Folge der digitalen Transformation ergeben, sollten vom Gedanken geleitet werden, dass diese Transformation die Grundwerte unserer Gesellschaftsordnung beeinflusst. Damit ist nicht gesagt, dass jede Veränderung der Interpretation dieser Grundwerte per se negativ zu werten ist. Es besteht aber grundsätzlich eine Beweislast auf Seiten jener gesellschaftlichen Kräfte, die durch konkrete digitale Innovationen bestimmte Werte tangieren, aufzuzeigen, wie diese Innovationen zum Gemeinwohl beitragen bzw. diesem nicht schaden. Diese abstrakte Forderung wird sich je nach Anwendungsfall unterschiedlich ausprägen. Sie bringt aber zum Ausdruck, dass der ethische Standpunkt bei der Beurteilung neuer digitaler Innovationen immer auch Beachtung finden soll. Insbesondere sollte die Digitalisierung im Sinne „digitaler Befähigung“ und informationeller Selbstbestimmung ausgestaltet werden. Entsprechend braucht es – im Sinne des Schutzes von Menschenwürde und Demokratie – dringend neue Lösungen und Instrumente zur Förderung der informationellen Selbstbestimmung.

Anregungen zur Konkretisierung dieser Massnahmen sind:

- Eine breite Nutzung digitaler Technologien zur Datengenerierung über grosse Teile der Bevölkerung darf das **Wahrnehmen der Grundrechte** nicht beeinflussen, also z.B. über den Zugang zu staatlichen Leistungen entscheiden (im Sinn eines „Citizen Score"). Es ist darauf zu achten, dass die Wahrnehmung von Grundrechten auch dann möglich ist, wenn Individuen bestimmte digitale Technologien (z.B. Smartphones) nicht nutzen wollen. Das geltende Rechtssystem ist bezüglich regulatorischer Sicherungen gegen solche Bestrebungen zu prüfen.
- **Probleme, welche sich aus der Nutzung digitaler Technologien ergeben** (z.B. verbesserte Effizienz von Propaganda) dürfen nicht in einer Art und Weise gelöst werden, welche Grundrechte einschränkt (z.B. Aufbau einer „Wahrheitsbehörde", welche darüber entscheidet, welche Form politischer Information wahr oder falsch ist).
- Jede Form von „**Nudging"** - ob mittels digitaler Mittel oder anderweitig – muss demokratisch legitimiert und transparent sein. Zudem soll regelmässig geprüft werden, ob die mit dem Nudging angestrebten Ziele auch erreicht werden, und die Öffentlichkeit ist entsprechend zu informieren. Erreicht eine Nudging-Mass-

nahme ihre Ziele nicht oder nur ungenügend, soll sie wieder abgebrochen werden.

- Die Nutzung von **automatisierten Entscheidungssystemen in sensiblen Bereichen** muss menschliche Entscheidungskapazität immer in geeigneter Weise einbinden (z.B. Möglichkeit einer „menschlichen Zweitmeinung"). Automatisierte Entscheidungssysteme in Bereichen, in denen ethische Dilemmata zu erwarten sind, sollten nur dann entwickelt werden, wenn sie die Wahrscheinlichkeit des Auftretens solcher Dilemmata deutlich vermindern.
- Effizienzgewinne durch digitale Technologien in grundrechtsrelevanten Bereichen rechtfertigen **keine Zwangsmassnahmen und physische Interventionen** in Individuen (z.B. eine mögliche Pflicht zur Implantierung eines Chips zwecks effizienter Identitätsüberprüfung).
- Forschung zur Entwicklung (digitaler) **Instrumente, welche die Wahrung der Grundrechte unterstützen**, ist zu fördern. Dies betrifft beispielsweise Instrumente für informationelle Selbstbestimmung oder die Entwicklung von Reputations-, Qualifikations- und Moderationsmechanismen.

Empfehlungen:

47. Bund und Kantone setzen sich dafür ein, dass der Schutz von Grundwerten, Menschenrechten und Menschenwürde auch im digitalen Zeitalter gesichert und die informationelle Selbstbestimmung gefördert werden.

48. Bund und Kantone sorgen in Zusammenarbeit mit den verantwortlichen Behörden und Anbietern im Bereich der Berufsausbildung dafür, dass die Ethik zu einem festen Bestandteil der Aus- und Weiterbildung wird, und nehmen diese Aspekte in ihre Erwartungen an das verantwortungsvolle Unternehmertum auf.

49. Bund und Kantone schaffen die Voraussetzungen dafür, dass Hochschulen und Weiterbildungseinrichtungen Forschung und Lehre in den Bereichen „Responsible Innovation“ (verantwortungsvolle Innovation) und „Design for Values“ (Werte-orientiertes Design) intensivieren.

50. Der Bund sorgt für ausreichende Transparenz, Nachvollziehbarkeit, Verständlichkeit und Accountability (Rechenschaftspflicht) bei digitalen Prozessen und Algorithmen, um eine vertrauensbasierte digitale Wirtschaft und Gesellschaft zu gewährleisten.

51. Der Bund schafft die nötigen rechtlichen Grundlagen, um sicherzustellen, dass bei elektronischer interaktiver Kommunikation transparent gemacht wird, wenn die Kommunikation nicht mit einem Menschen erfolgt.

12 Beilage 1: Zusammensetzung der Expertengruppe

Präsidentin:

lic.iur.Brigitta M. Gadient, LL.M., a. Nationalrätin

Wissenschaft/Forschung:

PD. Dr. Markus Christen, Universität Zürich

Prof. Dr. Nicolas Gisin, Professor Universität Genf

Prof. Dr. Dirk Helbing, Professor ETH Zürich

Prof. Jean-Pierre Hubaux, Professor ETH Lausanne

Dr. Matthias Kaiserswerth, früherer Direktor IBM-Forschungszentrum, Geschäftsführer Hasler Stiftung

Prof. Dr. Adrian Perrig, Professor ETH Zürich

Recht:

Prof. Dr. Rolf H. Weber, em. Professor Universität Zürich

Dr. Ursula Widmer, ehemalige Präsidentin Information Security Society (ISSS)

Wirtschaft:

Thomas Pletscher, Mitglied Geschäftsleitung Economiesuisse

Kommunikation/Gesellschaft:

Prof. Dr. Regula Hänggli, Professorin Universität Freiburg

Verwaltung:

Peter Fischer, Delegierter Informatiksteuerungsorgan Bund

Adrian Lobsiger, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (seit Juni 2016)

Prof. Dr. Luzius Mader, stellvertretender Direktor Bundesamt für Justiz

Hanspeter Thür, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (bis Ende 2015)

Sekretariat

Arié Malz (Leitung)

13 Beilage 2: Konsultierte Experten und Interessenvertreter

Dr. Thomas Dübendorfer
President, The Swiss ICT Investor Club (SICTIC), Zürich

Raoul Egeli
Präsident Schweizerischer Verband Creditreform, Vertreter des SGV

Dr. Alain Gut
Präsident der Kommission Bildung, ICTswitzerland

Franz Grüter
Nationalrat, Vize-Präsident ICTSwitzerland, CEO und Verwaltungsratspräsident der green.ch

Dr. Christian Kunz
Cofounder und CEO BitsaboutMe AG, Bern

Dale Kutnick
Senior Vice President and Director of Research; Gartner Inc. Stamford USA

Prof. Friedemann Mattern
Department of Computer Science, ETH Zürich

Patrick Schmid
Senior Account Executive; Gartner Inc. Switzerland

Sara Stalder
Geschäftsleiterin Stiftung für Konsumentenschutz (SKS)

Martin Vögeli
Leiter Group Strategy& Board Services, Swisscom

14 Beilage 3: Abkürzungsverzeichnis und Glossar

Advanced Persistent Threat (APT): Bezeichnet einen komplexen, zielgerichteten und langandauernden Angriff auf spezifische digitale IT-Infrastrukturen und vertrauliche Daten, wobei der Angreifer viele Ressourcen investiert.

Aktor: Antriebselement, das elektrische Impulse in mechanische Grössen umsetzt**.**

Anti Virus: Software, die bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspüren, blockieren und gegebenenfalls beseitigt

BEG: Bucheffektengesetz vom 3. Oktober 2008, SR **957.1**

BGA: Archivierungsgesetz vom 26. Juni 1998, SR **152.1**

BGÖ: Öffentlichkeitsgesetz vom 17. Dezember 2004, SR **152.3**

BGS: Geldspielgesetz vom 29. September 2017, SR… BBl **2017** 6245

Botnet: Auch als „Zombie-Netz“ bezeichnet ist eine Gruppe automatisierter Schadprogramme, sogenannter Bots. Dafür werden die Ressourcen vieler Computer in einem Netzverbund zusammengeführt und für Angriffe benutzt. Die Computer werden vorab vom Angreifer korrumpiert und ohne Wissen der Besitzer in diesen „Bots“ eingesetzt.

BSI: Bundesamt für Sicherheit in der Informationstechnik in Deutschland, zivile Bundesbehörde, welche für Fragen im Bereich der IT-Sicherheit zuständig ist

BSIG: Deutsches Gesetz über das Bundesamt (s. BSI) für Sicherheit in der Informationstechnik (s. BSI)

B2B: Interaktive Beziehungen zwischen Anbietern/Produzenten und anderen Produzenten und Anbietern.

B2C: Interaktive Beziehungen zwischen Anbietern/Produzenten und Konsumenten.

BÜPF: Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs, SR **780.1**

C&C: Command and Control sind Kontrollfunktionen in Botnetzen, die durch Command-and-Control-Server ausgeführt werden.

Cyber-physische Geräte (CPS): In CPS werden informations- und softwaretechnische Komponenten mit mechanischen bzw. elektronischen Bestandteilen verbunden. Durch die Einbindung von Sensoren und Aktoren in diese integrierten Systeme stellen CPS neuartige Systemfunktionen in Echtzeit für die Informations-, Daten-, und Funktionsintegration zur Verfügung. Das IoT baut auf CPS auf.

DDoS: Bei einem Distributed Denial of Service (DDoS)-Angriff wird eine große Zahl korrumpierter Systeme für den Angriff auf ein einzelnes Ziel mobilisiert. Das Ziel-System kann diesen Ansturm meist nicht bewältigen und ist dadurch für seine Nutzer nicht mehr erreichbar.

Deep Learning: Ist ein Untergebiet des Machine Learning. Zeichnet sich im Unterschied zum Machine Learning dadurch aus, dass das System mittels künstlicher neuraler Netzwerke selbst lernt, Unterscheidungsmerkmale zu erkennen und dann anzuwenden.

Deepnet bzw. Darknet: Teil des World Wide Web, das auf einem Peer-to Peer Netzwerk (Netzwerk gleichberechtigter Partner, die untereinander Verbindungen aufbauen) beruht. Das Deepnet bzw. Darknet stellt den bei weitem grösseren Teil des Netzes dar und entzieht sich den Suchmaschinen des Internets.

Differential Privacy: Anonymisierungsverfahren, bei dem die originalen Daten bei einer Anfrage durch so viele Dummys ergänzt werden (Rauschen), dass über einen Datensatz hinweg eine statistische Auswertung möglich ist, eine Identifizierung der Person jedoch nicht. Der Begriff fällt in den Bereich der sicheren Veröffentlichung von sensiblen Informationen. Mechanismen, welche die Anforderungen der differential Privacy erfüllen, verhindern, dass Angreifer unterscheiden können, ob eine bestimmte Person in einer Datenbank enthalten ist oder nicht.

Digital Divide: Bezeichnet den ungleichen Zugang zu Computern, Internet und Kommunikationstechnologien aufgrund von Armut oder anderer struktureller Ursachen z.B. Geschlecht oder das Fehlen von Sprachkenntnissen.

Disintermediation: Beschreibt den Ausschluss von Intermediären (Vermittler) in der Marktkette vom Ersteller des Produkts bzw. der Dienstleistung bis zum Verbraucher durch das Internet und moderne Kommunikationsmittel.

DSG: Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR **235.1**

DSGVO: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27 April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/36/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S.1

E-ID: Elektronische Identität.

EDÖB: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

FinfraG: Finanzmarktinfrastrukturgesetz vom 19. Juni 2015, SR **958.1**

Firewall: Aus Soft- und Hardware bestehende Sicherheitskomponente, die den ein- und ausgehenden Datenverkehr kontrolliert und einschränkt. Sie wird zum Schutz von digitalen Infrastrukturen (Computer, Netzwerke) eingesetzt und ist eine grundlegende Schutzmaßnahme, um ungewollte Netzzugriffe zu verhindern.

Freemium: Geschäftsmodell, bei dem die Basisdienste kostenlos angeboten werden, Erweiterungen bzw. das gesamte Serviceangebot konstenpflichtig sind.

Freenet: Peer-to-Peer-Software zum Aufbau eines Netzwerks, dessen Ziel darin besteht, Daten verteilt zu speichern und dabei Zensur zu vereiteln und anonymen Austausch von Informationen zu ermöglichen.

Geoblocking: Im Internet eingesetzte Technik, um Webseiten in definierten geographischen Gebieten zu sperren.

Gig Economy, auch Plattformökonomie genannt: Neuer im Zuge der Digitalisierung entstandener Teil des Arbeitsmarktes, bei dem in der Regel kurzfristige Aufträge auf Onlineplattformen ausgeschrieben werden. Die Adressaten der Aufträge sind selbständige Arbeitnehmer oder geringfügig Beschäftigte. Die Plattformbetreiber sind häufig Mittler zwischen Kunden und Auftragnehmern. Sie setzen die Rahmenbedingungen und behalten eine Provision für ihre Dienste. Beispiele sind Uber oder Upwork.

G2Ci (Government to Citizen): interaktive Beziehungen zwischen Behörden und Bürgern.

IAM: Identity and Access Management beschreibt ein zentralisiertes Sicherheitskonzept, das ganzheitlich die Administration der Zugriffsrechte und der betroffenen Identitäten sicherstellt.

IKT: Informations- und Kommunikationstechnik

IoE: Internet of Everything beschreibt die Verknüpfung zwischen Menschen, Prozessen, Daten und Gegenständen und stellt somit die Weiterentwicklung des Internets der Dinge (IoT) dar.

IoT: Internet of Things beschreibt die Vernetzung von netzwerkfähigen Gegenständen in einem universalen digitalen Netz, zumeist mit dem Internet. Die Geräte werden damit allgegenwärtig, bleiben aber trotzdem autonom. Das IoT verknüpft die Welt der Daten mit der Welt der Dinge.

I2P: Invisible Internet Project ist ein Open Source Projekt, das den Aufbau eines anonymen Netzwerkes für die Kommunikation im Netz erlaubt.

K-Anonymität: Verbreitetes wissenschaftliches Mass für den Grad der Anonymisierung von Daten. Wenn Datensätze, die zwecks Anonymisierung verändert wurden, nicht mehr einzelnen Personen, aber einer Personengruppe von K oder mehr Personen zugeordnet werden können, spricht man von K-Anonymität.

KG: Kartellgesetz vom 6. Oktober 1995, SR **251**

K 108: Datenschutzkonvention des Europarates (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten). Die europäische Datenschutzkonvention 108 hat als völkerrechtlicher Vertrag den Datenschutz natürlicher Personen zum Inhalt. Die Schweiz hat das Übereinkommen am 1. Februar 1998 in Kraft gesetzt (SR **0.235.1**)

L-Diversität: Mass für die Anonymisierung von Daten; enthält eine kleine, aber wesentliche Verfeinerung des Konzeptes der K-Anonymität. Die K-Anonymität ist als Anonymitätsmass nicht völlig verlässlich. L-Diversität stellt nun sicher, dass in einer K-Gruppe bei allen Merkmalen mindestens l verschiedene Merkmalsausprägungen vorkommen.

Machine Learning: Beruht auf Algorithmen, die oft statistische Ansätze der Datenbearbeitung nutzen, um Muster zu erkennen und daraus zu lernen.

MG: Militärgesetz vom 3. Februar 1995, SR **510.10**

MPLS: Multiprotocol Label Switching erlaubt den Transfer von Daten, wobei der Weg des Datenpakets anders als beim bekanntem IP-Netz vorab bestimmt ist. MPLS erlaubt den Aufbau geschützter abgetrennter Netze auf dem OSI-Layer zwei (Ethernet) mit Punkt zu Punkt Verbindungen.

M2M: Machine to Machine beschreibt den automatischen digitalen Informationsaustausch zwischen Maschinen/Endgeräten

NDG: Nachrichtendienstgesetz vom 25. September 2015, SR **121**

NIS: Richtlinie 2016/1148/EU des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz – und Informationssystemen in der Union, ABl. L 194 vom 19. Juli 2016

OGD: „Open Government Data“ verbindet das Konzept „Open Government“ als Leitbild staatlichen Handelns mit den Konzepten „Open Data“ und „Government Data“. Letztere stellen bestimmte Merkmale der Datenbereitstellung in den Vordergrund (aus der Open-Government-Data-Strategie Schweiz 2014–2018).

OR: Obligationenrecht, SR **220**

Outsourcing/Managed Services: Auslagerung von IT-Unternehmensaufgaben und -strukturen an externe Dienstleister.

PatG: Patentgesetz vom 25. Juni 1954, SR **232.14**

PBV: Preisbekanntgabeverordnung vom 11. Dezember 1978, SR **942.211**

Peer-to-Peer: In einem reinen Peer-to-Peer-Netz sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen als auch zur Verfügung stellen.

Perimeterschutz: Die Perimeter-Sicherheit betrifft die Sicherheit am Übergang zwischen einem Privat- oder Unternehmensnetz und einem öffentlichen Netz wie dem Internet. Perimeterschutz bildet eine erste Verteidigungslinie zum Schutz des eigenen Netzwerks gegen Cyberangriffe.

Phishing-Angriffe: Das Wort Phishing setzt sich aus den englischen Wörtern „Password", „Harvesting" und „Fishing" zusammen. Phishing beschreibt ein Angriffsmuster, bei dem durch den Versand von gefälschten E-Mails oder SMS Internet-Anwender auf gefälschte Internetseiten von Banken etc. geführt werden mit dem Ziel, Benutzererkennungen und Passwörter zu erhalten.

PrHG: Produktehaftpflichtgesetz vom 18. Juni 1993, SR **221.112.944**

Privacy by Design: Beim Datenschutz durch Technikgestaltung geht es darum, bereits bei der Erarbeitung eines Datenverarbeitungsvorgangs technische Massnahmen vorzusehen, die eine Verletzung des Datenschutzes verhindern. Dazu gehören etwa Massnahmen wie Anonymisierung, Verschlüsselung und Datenminimierung.

Privacy by Default: Datenschutzfreundliche Voreinstellungen müssen sicherstellen, dass nur Personendaten bearbeitet werden, deren Bearbeitung für den Verwendungszweck erforderlich sind.

Privacy Paradox: Einerseits geben die Nutzer immer mehr personenbezogene Daten (Name, Bilder, Mobile-Nummer, sogar religiöse Bekenntnisse) im Netz preis, andererseits ist ihnen der Schutz ihrer Privatsphäre wichtig. Bei genauerer Analyse ist dieses Phänomen aber nur scheinbar paradox, denn es gibt keinen signifikanten Zusammenhang zwischen Sorge um die eigene Privatsphäre und der Datenherausgabe. Eine Mehrheit scheint bei der Güterabwägung die Teilhabe am sozialen Leben im Netz zu priorisieren.

Privacy Shield: s. Safe-Harbor-Abkommen.

PrSG: Bundesgesetz vom 12. Juni 2009 über die Produktesicherheit; SR **930.11**

RetTech (Regulatory Technologie): Überbegriff für Massnahmen und moderne Technologien, welche Compliance und Risikomanagement unterstützen.

Ransomware: Schadsoftware, die Daten auf Computern verschlüsselt und nur gegen eine Zahlung wieder entschlüsselt.

RHG: Registerharmonisierungsgesetz vom 23. Juni 2006, SR **431.02**

RSA: Nach seinen Entwicklern Rivest, Shamir und Adleman benanntes asymmetrisches kryptografisches Verfahren. Wie auch andere asymmetrische Verschlüsselungsverfahren beruht RSA auf Einwegfunktionen.

Safe-Harbor-Abkommen: Die Gesetzgebung der USA gewährleistet aus Sicht der Schweiz keinen angemessenen Datenschutz. Um den Datentransfer zu erleichtern, haben die Schweiz und die USA ein Regelwerk erarbeitet, welches für die darunter zertifizierten US-Unternehmen ein ausreichendes Datenschutzniveau gewährleistet. Dieses Rahmenwerk wurde 2008 im Rahmen eines Briefwechsels geschaffen und 2017 durch „Privacy Shield“ ersetzt.

SchKG: Bundesgesetz vom 11. April 1889 über Schuldbetreibung und Konkurs, SR **281.1**

SDN: Software defined Networking ermöglicht eine Netzwerksteuerung auf der Stufe Software, die von der Hardware entkoppelt ist. Anders als in gewöhnlichen Netzwerken kann ein Administrator die Wege im Netzwerk für ein Datenpaket definieren.

SD-WAN: Software defined WAN (Wide Area Network) erlaubt den Aufbau eines weiten Netzes. Ähnlich wie beim SDN ermöglicht das System auf der Softwareebene ein Netzwerkmanagement, womit sich die Verbindungsstrukturen flexibel und nach spezifischen Sicherheitsprinzipien gestalten lassen.

SHA 256, 384: Secure Hash Algorithm sind standardisierte kryptografische Verfahren, die eine Hashfunktion (mathematisch hergeleitete Prüfsummen von einem beliebigen Wert) durchführen.

Security by Design: Grundlegendes Prinzip, wonach bereits bei der Entwicklung von Hard- und Software die Systeme so frei von Schwachstellen wie möglich und unempfindlich gegen Angriffe zu konzipieren sind.

Social Engineering: Direkte zwischenmenschliche Beeinflussung, um an vertrauliche Informationen zu gelangen oder die Opfer zu einem bestimmen Verhalten zu bewegen.

Tor (Akronym für The Onion Routing): Schützt seine Nutzer vor der Analyse des Datenverkehrs und ermöglicht dadurch einen weitgehend anonymen Zugang zum Internet.

U-ID: Einheitliche Unternehmens-Identifikationsnummer (UID) für alle in der Schweiz aktiven Unternehmen

URG: Urheberrechtsgestz vom 9. Oktober 1992, SR **231.1**

UWG: Bundesgesetz vom 19. Dezember 2013 gegen den unlauteren Wettbewerb, SR **241**

VEleS: Verordnung der Bundeskanzlei über die elektronische Stimmabgabe, SR **161.116**

Vulnerabilities Scan: Verwundbarkeitsüberprüfung von digitalen Infrastrukturen mit dem Ziel, bekannte Sicherheitslücken und nicht konformes Verhalten der Systeme zu erkennen.

Zero-Day Exploit: Angriff, der zum ersten Mal eine Schwachstelle in Hard-, vor allem aber Software nutzt.

ZertES: Bundesgesetz vom 18. März 2016 über die elektronische Signatur, SR **943.03**

ZGB: Zivilgesetzbuch, SR **210**

15 Beilage 4: Standards und Meldepflichten im Ländervergleich

Einleitung

Die rasante Zunahme und Abhängigkeit von digitalen Infrastrukturen sowie deren Wichtigkeit für die Gesellschaft konfrontieren das Staatsgefüge mit vielfältigen Herausforderungen. Insbesondere stellt sich die Frage, wo und wie der Staat intervenieren soll, um die Chancen und Risiken der digitalen Transformation in geordnete Bahnen zu lenken. Der folgende Ländervergleich zeigt, wie in anderen Staaten die verschiedenen kritischen Infrastrukturen und relevanten Online-Dienste reguliert sind und welche Stossrichtungen verfolgt werden.

Umfang der Auswertung

Die Auswertung beruht auf einer Umfrage, welche die Expertengruppe mit Unterstützung des EDA und von zwölf EDA-Aussenstellen durchführen konnte.[25] Die aus den Rückmeldungen erstellte Übersicht zeigt die Situation von staatlichen Vorgaben zu IKT-Sicherheitsstandards in folgenden Ländern auf: Deutschland, Österreich, Frankreich, Grossbritannien, Schweden, Norwegen, Finnland, Singapur, Hongkong, Australien, China sowie Vereinigte Staaten von Amerika.

Situation im europäischen Raum

Allgemein gelten bei europäischen Staaten die verpflichtenden Vorgaben durch NIS. NIS gilt für kritische Infrastrukturen und den Digital Communication Sektor. Die EU-NIS ist eine Richtlinie und muss von den Mitgliedstaaten mit einem entsprechenden Gesetzeswerk ins Landesrecht überführt werden. Zum Auswertungszeitpunkt war die Umsetzung noch nicht von allen Mitgliedstaaten vollzogen.

Deutschland verfügt seit Juli 2015 über ein nationales "IT-Sicherheitsgesetz", welches sich an die Betreiber von kritischen Infrastrukturen (KRITIS) richtet. Dies sind Einrichtungen, Anlagen oder Teile, welche den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser und Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Die KRITIS-Betreiber werden durch Rechtsverordnung definiert und verpflichten sich zur Einhaltung von technischen Mindeststandards sowie einer Meldepflicht. Als staatliche Stelle nimmt das Bundesamt für Sicherheit in der Informationstechnik BSI eine Vielzahl von Aufgaben wahr und hat dabei weitreichende Kompetenzen im Zusammenhang mit der Informationssicherheit auf nationaler Ebene (§ 3 BSIG). Beispielsweise können Betreiber kritischer Infrastrukturen und ihre Branchenverbände dem BSI branchenspezifische Sicherheitsstandards vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen zu gewährleisten. Betreiber kritischer Infrastrukturen haben zudem mindestens alle zwei Jahre die Erfüllung der Anforderungen nachzuweisen.

Konkrete Sicherheitsstandards existieren durch die spezifischen rechtlichen Grundlagen für öffentliche Telekommunikationsnetze (TKG), Energieversorgungsnetze (EnWG), Energieanlagen (EnWG), Kernkraftwerke und atomare Lager (Atomgesetz).

[25] Die Expertengruppe dankt dem EDA für die gute und wertvolle Zusammenarbeit, ohne die diese Länderübersicht nicht hätte erstellt werden können.

In **Österreich** sieht der Entwurf für das „Netz- und Informationssystemsicherheitsgesetz“ (NIGS) zukünftig vor, dass für die Betreiber wesentlicher Dienste verpflichtende Sicherheitsstandards erlassen werden (Verordnung des Bundeskanzlers). Die NIS-Richtlinie[26] unterscheidet zwischen Betreibern wesentlicher Dienste (Sektoren in Fussnote angeführt[27]) und Anbietern digitaler Dienste (i.S. der Richtlinie 2015/1535/EU). Das geplante NISG wird dieser Systematik folgen. Analog sieht auch das „Österreichische Programm zum Schutz kritischer Infrastrukturen Masterplan 2014“ (APCIP) die Entwicklung von Sicherheitsstandards vor (auch für den Bereich IKT). Das APCIP ist zurzeit noch nicht umgesetzt, da auf die Standards des NISG gewartet wird. Auch sieht der Entwurf des NISG eine Meldepflicht für die Betreiber wesentlicher Dienste und Anbieter bei Sicherheitsvorfällen vor. Hierzu wird eine Meldestelle in der operativen NIS-Behörde eingerichtet. Der gesetzlichen Meldepflicht unterliegen ergänzend auch KMU oder NPO, wenn diese als Betreiber wesentlicher Dienste ausgewiesen sind. Das NISG, einschließlich der dort festgelegten Standards, wird auch für die öffentliche Verwaltung gelten. Bei gewissen strategischen Unternehmen, welche als kritische Infrastrukturen ausgewiesen sind, besteht zwar keine gesetzliche Meldepflicht, sie sind jedoch angehalten, Sicherheitsvorfälle der Kontakt- und Meldestelle im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) zu melden. Dazu unterzeichnen das BVT und die Betreiber Kooperationsvereinbarungen über den Austausch klassifizierter Informationen.

Durch die „Agence nationale de sécurité des systèmes d'information“ (ANSSI) werden in **Frankreich** seit Juli 2016 Vorschriften publiziert, welche die Betreiber „kritischer Infrastrukturen" zu Schutzmassnahmen verpflichten. Zu den ersten Sektoren zählen hierbei Gesundheit, Lebensmittel und Wasserwirtschaft, wobei weitere folgen sollen. Hervorzuheben ist, dass ca. 250 staatliche und nichtstaatliche Betreiber den Vorschriften unterliegen und die Liste der Betreiber vertraulich ist. Diese Gesetzesgrundlage wurde im Zuge des französischen Militärplanungsgesetzes vom Dezember 2013 geschaffen. Die von den Vorgaben betroffenen ca. 250 Betreiber kritischer Infrastrukturen unterliegen dabei gegenüber ANSSI einer Informations- und Meldepflicht für vordefinierte Vor- bzw. Zwischenfälle.[28] Für Institutionen, welche nicht der vorgängig erwähnten Verpflichtung angehören, besteht zurzeit keine Meldepflicht gegenüber ANSSI. Mit der Umsetzung von NIS dürfte sich die Zahl der neu der ANSSI-Vorgaben unterstehenden Betreiber jedoch auf weitere Sektoren ausweiten.

Grossbritannien ist zurzeit national an der Erarbeitung und Einführung von NIS. Die Umsetzung und Ausgestaltung der NIS-Vorgaben obliegt dabei verschiedenen staatlichen Akteuren.[29] Allgemein existieren bereits gewisse IKT-Sicherheitsvorgaben, wel-

[26] Zur Umsetzung der Richtlinie 2016/1148/EU vom 6. Juli 2017 (NIS-Richtlinie) wird in Ö ein Netz- und Informationssicherheitsgesetz (NISG) vorbereitet.

[27] Zu den wesentlichen Diensten zählen gemäss NIS Anhang II: Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasserlieferung und –versorgung, digitale Infrastruktur (IXPs, DNS-Dienstanbieter, TLS-Name-Registries).

[28] Les opérateurs d'importance vitale (OIV) sont obligés de transmettre différentes informations: 1) des déclarations d'incidents; 2) une "cartographie" de leurs systèmes d'information d'importance vitale; 3) un tableau de bord de suivi de certains indicateurs de sécurité des systèmes d'information.

[29] „Department for Digital, Culture, Media & Sport“, des Cabinet Office, des Governement Digital Service sowie des Department for Business, Energy & Industrial Strategy.

che vom „National Cyber Security Center“ (NCSC) erarbeitet wurden. Diese „Guidelines“ verstehen sich in erster Linie als Hilfestellung im ICT-Security-Bereich der staatlichen Administration (government departments, agencies) sowie der nationalen kritischen Infrastrukturen. Die Guidelines sind auch relevant für die lokalen Administrationen (local government) und den erweiterten öffentlichen Sector (wider public sector). Inwiefern die „Guidelines“ verpflichtenden Charakter ausweisen, lässt sich nicht beurteilen.

Situation im skandinavischen Raum

Schweden erlässt zurzeit keine verpflichtenden staatlichen Vorgaben für die Betreiber von „Digitaler Infrastruktur“ und „Online-Diensten“. Für die Betreiber „Kritischer Infrastruktur“ weist die staatliche "Swedish Civil Contingencies Agency” (MSB) jedoch insbesondere auf die Berücksichtigung von etablierten Methoden und Standards der ISO-27k-Reihe hin. Soweit ersichtlich besteht für die vorgängig erwähnten Betreiber – mit Ausnahme gewisser Sektoren - keine obligatorische Meldepflicht bei Zwischenfällen. Eine gewisse Meldepflicht ergibt sich aus bestehenden Schutzgesetzgebungen (beispielsweise für die Sektoren Elektrizität und Telekommunikation).[30] Staatliche Betreiberinstitutionen sowie die Verwaltung sind jedoch verpflichtet, der MSB Zwischenfälle zu melden.

In **Norwegen** geben die staatlichen Behörden eine Reihe von Empfehlungen und Anforderungen im Bereich der IKT-Sicherheit heraus. Diese werden schwergewichtig sektoriell durch die zuständigen Ministerien erlassen. Dabei erlässt der Staat sowohl verpflichtende Empfehlungen wie auch Empfehlungen mit Richtliniencharakter. Eine gewisse Meldepflicht ergibt sich aus dem „National Security Act“. Dieser verpflichtet die verschiedenen Ministerien, dem Justizministerium einen jährlichen Statusbericht in Bezug auf die Einhaltung der Vorschriften in ihrem Sektor zuzustellen.

In **Finnland** ist die „Finnish Communications Regulatory Authority” (FICORA) ermächtigt, im Telekommunikationssektor Vorschriften über Informationssicherheit zu erlassen. Die Koordination zwischen FICORA und dem Telekommunikationssektor erfolgt in Zusammenarbeit mit dem "National Cyber Security Centre“ (NCSC-FI). Telekommunikationsanbieter sind verpflichtet FICORA über allfällige Sicherheitsvorfälle in ihren Netzwerken zu informieren. Im Bereich der kritischen Infrastrukturen bietet die „National Emergency Supply Agency“ (NESA) den Betreibern mittels Leitlinien zur Informationssicherheit eine gewisse Hilfestellung. Soweit ersichtlich, haben die Anleitungen des NCSC-FI für die Betreiber keinen verbindlichen Charakter. Generell ist jedoch anzunehmen, dass sektoriell die dafür zuständigen Ministerien Empfehlungen mit verbindlichem Charakter erlassen, insbesondere in der Verwaltung. Mit der Umsetzung von NIS ist davon auszugehen, dass die Betreiber kritischer Infrastrukturen sowie weitere Sektoren einer obligatorischen Meldepflicht bei Informationssicherheitsvorfällen unterliegen werden.

[30] Incident reporting in the telecoms sector (EU telecoms package Article 13a).

Situation im asiatischen Raum und in Australien

Generell existieren in **China** für Betreiber digitaler Infrastruktur und Online-Dienste gewisse IKT-Sicherheitsstandards, welche sich auch auf weitere Sektoren anwenden lassen. Inwieweit und in welchem Umfang eine obligatorische Meldestelle bei relevanten IT-Sicherheitsvorfällen besteht, ist aufgrund komplexer nationaler Bestimmungen im heutigen Zeitpunkt nicht eindeutig zu beurteilen. Erschwert wird das Ganze auch dadurch, dass sich zwei Regierungs-Institutionen um die strategische und operative Entscheidungsbefugnis bemühen.[31] Unabhängig davon lässt sich feststellen, dass tendenziell Organisationen mit ausländischem Einfluss einer erweiterten Prüfung in Bezug auf IKT- und Informationssicherheitsstandards unterliegen und sich entsprechend nach staatlichen Vorgaben ausrichten müssen

Die Regierung von **Hongkong** verabschiedete bis heute verschiedene umfassende Bestimmungen zur Thematik der Informationssicherheit. Bei der Entwicklung und Ausarbeitung umfassender Sicherheitsdokumente, einschließlich der Sicherheitsvorschriften, Richtlinien, Anweisungen und Verfahren, stützte sie sich dabei oftmals auf bereits bewährte Standards (ISO, Standards der „International Electrotechnical Commission“, usw.) ab. Diese Regelungen haben einen obligatorischen Anwendungscharakter für alle staatlichen Organisationseinheiten. Das “Government Computer Emergency Response Team Hong Kong” (GovCERT.HK) agiert hierbei als Koordinations- und Meldestelle für Informationsvorfälle im Cyberbereich. Alle staatlichen Organisationen (Betreiber kritischer wie auch nichtkritischer Infrastrukturen) unterstehen gegenüber dem GovCERT.HK einer Meldepflicht. Zudem stellt das Hong Kong Computer Emergency Response Team Coordination Centre” (HKCERT) im Sinne einer öffentlichen Informationsstelle allgemein präventive und sensibilisierende Dienstleistungen weiteren Akteuren wie lokalen KMU usw. zur Verfügung.

In **Singapur** trägt die "Cyber Security Agency of Singapore" (CSA) die alleinige Verantwortung, alle Aspekte im Zusammenhang mit Cybersicherheit zu koordinieren und zu überwachen. Generell verfolgt die Regierung von Singapur bei Regulierungen und Vorgaben einen „Top-down“-Ansatz, was zur Folge hat, dass die CSA mit weitreichenden Aufgaben, Verantwortlichkeiten und Kompetenzen ausgestattet ist[32]. Der „Cyber Security Act“ regelt die Vorgaben für Betreiber von kritischen Infrastrukturen. Das Rahmengesetz ist Sektoren übergreifend und Teil des National Security Masterplan 2018. Es gibt Mindestanforderungen für Vorbeugemassnahmen vor und soll der CSA die gesetzliche Grundlage geben. Singapur hat elf aus Staatssicht sicherheitsrelevante Sektoren definiert. In diesen Sektoren obliegt die Aufsicht zu sicherheitsrelevanten Aspekten usw. der jeweils verantwortlichen Behörde. Im Finanzsektor ist dies beispielsweise die „The Monetary Authority of Singapore“ (MAS). Sie legt entsprechend in den „Technology Risk Management Guidelines“ Richtlinien zur generellen Handhabung von Technologie- und Cyberrisiken im Finanzsektor fest. Generell müssen die verschiedenen Sektoren, wie auch die Verwaltung, Informationssicherheitsvorfälle der CSA weitermelden.

[31] The Chinese Administration for Cyber Security and the Ministry of Public Security are struggling for the strategic and operational decision-making power in the said field.

[32] Aufgaben der CSA: "also empowered to develop and enforce cybersecurity regulations, policies, and practices. It will coordinate efforts across government, industry, academia, businesses and the people sector, as well as internationally".

Australien verfügt mit dem „Cyber Security Center“ (ACSC) über eine Institution, welche für die Koordination von Behörden, Regulatoren und dem Privatsektor zuständig ist. Das ACSC sammelt Informationen, evaluiert Bedrohungen und berät den Privatsektor entsprechend. Ferner wurden innerhalb des „Federal Attorney-General’s Department“ zwei Institutionen ins Leben gerufen, welche eine Kooperation mit Betreibern kritischer Infrastrukturen sicherstellen. Das „Computer Emergency Response Team” (CERT), welches in enger Zusammenarbeit mit weiteren staatlichen Behörden agiert, ist dabei schwergewichtig Anlaufstelle bei Sicherheitsvorfällen im erwähnten Sektor. Die Aufgabe des CERT besteht darin, den Betreibern und Institutionen von nationalem Interesse nützliche, wirksame und rechtzeitige Ratschläge zur Vermeidung von Cyberangriffen zu vermitteln. Soweit ersichtlich besteht keine obligatorische Meldepflicht für Sicherheitsvorfälle. Im Sinne eines koordinierenden Gremiums wird durch das „Trusted Information Sharing Network“ (TISN) ein regulärer Informationsaustausch zwischen Betreibern kritischer Infrastrukturen, weiteren Sektoren sowie Staatsbetrieben gewährleistet.[33] Als Beispiel sei hier die „Australian Securities and Investment Commission“ (ASIC) erwähnt, welche für die Regulierung des Finanzsektors zuständig ist. Verbindliche staatliche Vorgaben zu ICT Security Standards existieren keine, da erwartet wird, dass die Banken angemessene Vorkehrungen im Rahmen ihres Risikomanagements treffen.

Situation in den USA

In den **Vereinigten Staaten von Amerika** sind verschiedene staatliche Departemente für den Bereich der Informationssicherheit verantwortlich. Entsprechend sind die verschiedenen Aufgaben, Verantwortlichkeiten und Kompetenzen im Zusammenhang mit einer staatlichen Vorgabe von IKT-Sicherheitsstandards sehr komplex aufgestellt. Eine koordinierende bzw. zentrale Rolle dürfte dabei dem „Department of Homeland Security“ (DHS) zugewiesen sein. Es darf davon ausgegangen werden, dass insbesondere bei Zwischenfällen, welche die Nationale Sicherheit betreffen, eine obligatorische Meldepflicht besteht. Nebst dem DHS ist davon auszugehen, dass auch sektoriell die zuständigen Ministerien zu einem gewissen Grad verbindliche Empfehlungen im Bereich IKT-Sicherheitsstandard erlassen. Allgemein existieren für Betreiber „Digitaler Infrastruktur“ und „Online-Dienste“ keine staatlichen IKT-Sicherheitsstandards. Im Bereich der Betreiber kritischer Infrastrukturen dürften jedoch sektoriell durch die zuständige Behörde Vorgaben erlassen werden, analog auch für die staatlichen Verwaltungseinheiten. Als Beispiel sei hier das „National Institute of Standards and Technology“ (NIST) erwähnt, welches mit dem sogenannten Cyber-Security Framework relativ detaillierte Quasi-Standards für die kritischen Infrastrukturen vorsieht.

[33] The sector groups include banking and finance, health, food and grocery, transport, energy, communications, water services and Commonwealth Government services.

Tabelle „Ländervergleich“

	Verpflichtende staatliche IKT-Standards für						
Staaten	Betreiber von „Digitale Infrastruktur“ und „Online-Dienste“	Melde-stelle	Alle Betreiber von „Kritische Infrastruktur“	Melde-stelle	„Verwaltung“	„Spezifische Sektoren“	Meldestelle
Schweiz	**A**	**A**	**A**	**A**	**AAA**	**AA**	**AA**
Deutschland	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AA**
Österreich	**AAA**	**AA**	**AAA**	**AA**	**AAA**	**A**	**AA**
Frankreich	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**
Grossbritannien	**A**	**A**	**AA**	**AA**	**AA**	**AA**	**AA**

Schweden	**A**	**A**	**AA**	**AA**	**AA**	**AAA**	**AAA**
Norwegen	**AA**	**A**	**AA**	**AA**	**AA**	**AA**	**AA**
Finnland	**AA**	**AA**	**AA**	**AA**	**AAA**	**AA**	**AA**
Singapur	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**
Hongkong	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**
Australien	**AA**	**AA**	**AA**	**AA**	**AA**	**AA**	**AA**
USA	**A**	**A**	**AA**	**AA**	**AAA**	**AAA**	**AAA**
China	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**

Anmerkung: Alle der analysierten Staaten verfügen derzeit über eine nationale Cyber-Strategie. Je nach Land sind die Bestrebungen in Bezug auf staatliche Vorgaben oder einer Meldestelle institutionell, rechtlich oder auch sektoriell sehr unterschiedlich ausgelegt. Die in der Tabelle dargestellte „Gewichtung“ zeigt die „tendenzielle Stossrichtung“ der staatlichen Vorgaben auf.

Das entsprechende Land verfügt über: **AAA = *„ausgeprägte“*** **AA = *„wenige“*** / **A = *„keine“*** bzw. ***„sehr wenige“*** Vorgaben oder Meldestelle/n