Deutsches Institut für Vertrauen und Sicherheit im Internet

DIVSI magazin

OKTOBER 2018

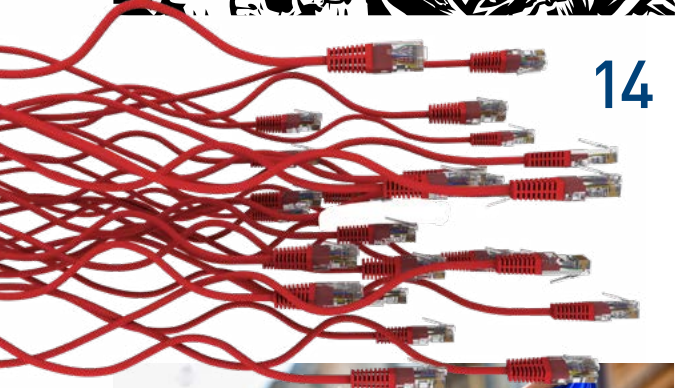
中国正在数据化道路上全速超车*

*China befindet sich bei der Digitalisierung voll auf der Überholspur

Und wie sieht es in Deutschland aus?

Schutz der digitalen Infrastrukturen gefordert.

Sichtbar geworden ist ein strategisches Defizit.



Inhalt

Impressum

Herausgeber:
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Matthias Kammer, Direktor
Mittelweg 110B
20149 Hamburg

Chefredakteur:
Jürgen Selonke (V.i.S.d.P.)

Autoren:
Jost Blöchl, Chenchao Liu, Dr. Florian Kessler, Dr. Konstantin von Notz, Dr. Kristin Shi-Kupfer, Prof. Dr. Friedrich Graf von Westphalen, Dr. Göttrik Wewer

Realisierung:
Lohrengel Mediendesign
Schulterblatt 58
20357 Hamburg

Verbreitete Auflage:
ca. 7.500 Exemplare, Abgabe kostenlos

Titel: May_Chanikran/vector-sector – shutterstock.com

Haben Sie Fragen oder wünschen weitere Informationen?

Web: www.divsi.de
E-Mail: info@divsi.de

Anfragen DIVSI magazin:
Michael Schneider,
Leitung Kommunikation
Tel.: + 49 40 226 369 895
E-Mail: michael.schneider@divsi.de
E-Mail: presse@divsi.de

Wissenschaftliche Leitung:
Joanna Schmölz
Tel.: + 49 40 226 369 896
E-Mail: wissenschaft@divsi.de

DIVSI ist eine gemeinnützige Initiative der Deutsche Post AG, gegründet im Jahr 2011.

Von Schlaglichtern auf China, einer Charta für Europa und Strategien für Deutschland

Der Optimist lernt Russisch, der Pessimist Chinesisch. Eine früher oft gegebene Antwort auf die Frage junger Menschen, welche Sprache sie lernen sollten. Ich habe deshalb einst ein Sinologie-Studium begonnen und leider – sage ich heute – abgebrochen, weil mich die Zeitungswelt stärker faszinierte.

Nicht dass ich meine Berufswahl bereue. Doch es wäre prima, fundierter über die Verhältnisse des Landes in Fernost Bescheid zu wissen. Man muss deshalb sicher kein Pessimist sein, sondern einfach Realitäten anerkennen.

Die Idee, ein Magazin mit dem Schwerpunkt China zu gestalten, entstand beim letzten DIVSI-Bucerius Forum. Einen besonderen Dank möchte ich den Experten von MERICS (Mercator Institute for China Studies) sagen, die auch für die Übertragung des Titels in chinesische Schriftzeichen gesorgt haben.

Insgesamt wecken die Beiträge mit Blick auf China Neugier, machen vielleicht zumindest teilweise auch Angst. Aber sie werfen Schlaglichter auf Themen, die eine Vertiefung lohnen.

Dabei setzt Kristin Shi-Kupfer ein Zeichen, das viele überraschen mag. Demnach geht in China längst nicht alles vom Staat aus. Die MERICS-Expertin zeichnet vielmehr ein Bild der chinesischen Gesellschaft als Treiber der Digitalisierung und informiert über anspruchsvolle Konsumenten sowie selbstbewusste Start-up-Unternehmer (S. 4).

Florian Kessler und Jost Blöchl, Rechtsanwälte des Pekinger Büros der Kanzlei WZR, schildern Wirkungen und Auswirkungen des chinesischen Cybersecurity-Gesetzes. Und benennen auch die wichtigsten To-Dos für ausländische Unternehmen (S. 14).

Wie aktiv die Chinesen im Bereich E-Health unterwegs sind, berichtet Chenchao Liu. Er informiert über den Einsatz künstlicher Intelligenz im Gesundheitswesen und verdeutlicht, dass man durchaus einen länderübergreifenden Nutzen im Auge hat (S. 10).

Und wie sieht es in Deutschland aus? Mit dem besonderen Blick auf IT-Sicherheit findet der Grünen-Spitzenpolitiker Konstantin von Notz viel Kritikwürdiges. Er geht mit der Bundesregierung hart ins Gericht und schlägt zwingend notwendige Maßnahmen vor (S. 24).

Göttrik Wewer zeigt, dass zwar einiges geschafft wurde, jedoch vor allem ein strategisches Defizit herrscht. Er schildert, worauf es jetzt ankommt (S. 22).

Informationen von Friedrich Graf von Westphalen zur aktuellen „Charta der Digitalen Grundrechte der Europäischen Union" runden das Spektrum des Magazins ab. Diese Leitlinie zeigt Wege auf, um Bedrohungen unserer Grundrechte durch die Digitalisierung entgegenzuwirken. Zumindest unter diesem Aspekt dürften wir den Chinesen voraus sein (S. 18).

Ich bin sicher, dass unsere aktuellen Themen Ihnen einmal mehr informative Unterhaltung bieten.

Jürgen Selonke
Chefredakteur, DIVSI magazin

Chinas Gesellschaft als Treiber der Digitalisierung

Anspruchsvolle Konsumenten und selbstbewusste Start-up-Unternehmer.

Kristin Shi-Kupfer

Es war eine Nachricht, die scheinbar so gar nicht zu der hiesigen Aufregung über Chinas digitale Entwicklung passen wollte. Chinesische Konsumenten, hierzulande vor allem als enthusiastische Nutzer neuer Technologien bekannt, probten einen kleinen Aufstand.

Anfang August machten sich Tausende wütender Kleinanleger aus dem ganzen Land auf in Richtung Finanzdistrikt im Westen Beijings. Sie wollten ihrem Frust über das Geld, das sie an windige Betreiber von Online-Kreditplattformen (auch Peer-to-Peer oder P2P genannt) verloren hatten, Luft machen. Und sie wollten die chinesische Zentralregierung in die Pflicht nehmen, das verlorene Geld zurückzuerstatten. Größere Proteste konnten die chinesischen Behörden letztlich verhindern – durch einen koordinierten Polizeieinsatz vor Ort, vor allem aber auch mithilfe des zunehmend umfassenderen digitalen Überwachungsnetzes. Womit die Wahrnehmung des Westens wiederhergestellt war: China ist eine globale Cybermacht, die ihre Bürger mit digitalen Techniken kontrollieren will.

Was bei dieser Wahrnehmung oft übersehen wird: Chinas Bevölkerung ist nicht nur ein willliger Empfänger, sondern auch Mitgestalter und oftmals sogar Treiber der Digitalisierung in der Volksrepublik. Wie die chinesische Zentralregierung ihre digitalen Ambitionen in punkto innovationsgetriebenes Wachstum, effizientes Regieren und globale Technologieführerschaft vorantreiben kann, wird deshalb entscheidend vom Verhalten der chinesischen Bevölkerung abhängen. Jüngste Trends zeigen, dass Chinas Gesellschaft die digitale Politik der Zentralregierung durchaus herausfordert.

Beispiel 1: Die eingangs erwähnten Kleininvestoren. Mit der Freigabe der Peer-to-Peer-Plattformen setzte die chinesische Regierung auf ein altbewährtes Mittel der Innovations- und Wachstumsförderung. 2015 riefen Ministerpräsident Li Keqiang und der damalige Zentralbankchef Zhou Xiaochuan die Plattformen ins Leben – ohne jedoch große, umfassende gesetzliche Rahmenbedingungen aufzusetzen. Die Dynamik des digitalen Marktes sollte eine vitale Finanzierungsquelle für kleine und mittelständische Unternehmen in China schaffen.

Das gelang auch zunächst teilweise: Die Zahl der Plattformen verzehnfachte sich innerhalb von nur drei Jahren. China ist heute der weltweit finanzkräftigste P2P-Markt. Auch aus Mangel an Alternativen für lukrative Geldanlagen entstanden durch die P2P-Plattformen eine Art Geldrausch. In der Hoffnung auf schnel- →

Fotos: atiger/saclad – Shutterstock

Angekommen. Chinas Bevölkerung ist auch Treiber der Digitalisierung.

Blick nach vorn.
Die neue Revolution.
Alle miteinander,
das Handy fest in
der Hand.

Fotos: University at Buffalo, sacilad/yuyangc – Shutterstock

→ les, großes Geld und im Vertrauen auf staatliche Rückendeckung ließen sich Anleger auf immer aberwitzigere Zinsraten ein, an welchen die Betreiber kräftig mitverdienten. Kreditnehmer konnten die entsprechenden Rückzahlungen bald nicht mehr leisten, gefährliche Verschuldungsketten entstanden, an deren anderem Ende die Kleinanleger festsaßen.

Schließlich musste die Zentralregierung aktiv werden: Sie schloss viele unseriöse und betrügerisch agierende Plattformen und unterstellte den gesamten Bereich einer zentralen Clearing-Stelle. Die zukünftige Herausforderung: Wie kann die Zentralregierung die Rahmenbedingungen für nachhaltige digitale Marktmechanismen schaffen und dabei Wildwest-Mechanismen verhindern – ohne ein unabhängiges Rechtssystem und aufklärende Medienberichterstattung?

Beispiel 2: Der Schutz privater Daten. Sowohl chinesische offizielle Medienberichte als auch Studien ausländischer Wissenschaftler kommen zu dem Ergebnis, dass Chinesen entweder keine, oder wenn doch, eine durchaus positive Einstellung zum sogenannten sozialen Bonitätssystem haben. Bis 2020 will die chinesische Zentralregierung ein umfassendes nationales System zur Bewertung von Zahlungsmoral, Verkehrsverhalten oder Online-Gewohnheiten einführen. Lokale Pilotprojekte mit „Schwarzen Listen" und kommerzielle Modelle für je nach Punktzahl erlaubte Zugänge, zum Beispiel zu Reisebuchungen, existieren bereits. Laut der Berichte und Studien zeigt sich eine Mehrheit überzeugt von dem Argument der Regierung, dass mithilfe von Gesichtserkennung und Datenanalyse Verbrecher und Unruhestifter gefasst und die Gesellschaft sicherer gemacht würde.

Eine im März dieses Jahres durchgeführte Umfrage des staatlichen Fernsehsenders CCTV und des Unternehmens Tencent Research unter rund 8.000 Teilnehmern zeigt jedoch auch einen anderen Trend: 76,3 Prozent der Teilnehmer sehen im Vormarsch von Methoden der Künstlichen Intelligenz (KI) in der IT eine Gefahr für ihre Privatsphäre. Rund ein Drittel (31,7 Prozent) fühlt sich bereits in der ein oder anderen Form bedroht. Und das, obwohl Peking KI zum Allheilmittel für fast alle Probleme ausgerufen hat und die eigene Forschung und Entwicklung in diesem Bereich mit massiven Investitionen vorantreibt.

> Wenn Nutzer Privatsphäre gegen Bequemlichkeit, gegen Sicherheit, gegen Effizienz tauschen können, dann tun sie das in vielen Fällen.
>
> **Robin Li, CEO des Suchmaschinenbetreibers Baidu**

Entrüstung. Auch brach ein Sturm der Entrüstung unter Chinas Netizens los, als der Chef des chinesischen Suchmaschinenbetreibers Baidu, Robin Li, ebenfalls im März dieses Jahres erklärte: „wenn Nutzer Privatsphäre gegen Bequemlichkeit, gegen Sicherheit, gegen Effizienz tauschen können, dann tun sie das in vielen Fällen". Zwei Monate zuvor hatte das halb staatliche Komitee für Konsumentenschutz in der östlichen Provinz Jiangsu die Firma Baidu wegen illegalen Sammelns von Daten angeklagt. Baidu entschuldigte sich, ohne aber rechtliche Konsequenzen zu tragen.

Die zunehmende Sensibilität vieler Chinesen für Belange des Datenschutzes ist begründet: Denn trotz einer Reihe von jüngst verabschiedeten gesetzlichen Regelungen, die hauptsächlich Firmen und weniger Regierungsstellen in die Verantwortung nehmen, hat die Zahl →

Social Scoring. Die lückenlose Erfassung des Lebens wird Einfluss auf den Alltag der Menschen haben. Doch viele Bürger finden das sogar gut.

Abschied vom Vorbild. Jack Ma, Gründer von Alibaba, hat überraschend seinen Rücktritt angekündigt. Man darf gespannt sein, wie sich sein Imperium jetzt weiterentwickelt.

→ von Datenschutzverletzungen in der Volksrepublik zugenommen: 2017 waren nach Erhebungen der chinesischen Forschungseinrichtung Internet Society of China rund 80 Prozent der chinesischen Internet-Nutzer von Datenverlusten (data leaks) betroffen. Es bleibt zu beobachten, wie sich das Bewusstsein und die Möglichkeiten von chinesischen Nutzern in Bezug auf Datenschutz entwickelt, wenn das soziale Bonitätssystem weiter Gestalt annimmt.

Beispiel 3: Die zunehmend selbstbewussten Start-up-Unternehmer. Die chinesische Gesellschaft ist vom Gründungsfieber gepackt. Mit einem eigenen Produkt Erfolg zu haben, ist für viele junge Chinesen attraktiver, als für andere zu arbeiten oder gar ein Leben lang Beamter zu sein. Viele wagen den Schritt in die Selbstständigkeit und bringen dabei einige Jahre Erfahrung und Netzwerke aus der IT-Branche mit. Sie tummeln sich am liebsten im Bereich der sogenannten Online-to-Offline-Dienste (O2O), wie beispielsweise Service-Apps für Essenslieferungen, oder im E-Commerce.

In großen Städten können angehende Gründer dabei in Hightech- und Kreativ-Parks Fuß fassen, die von lokalen Regierungen initiiert und bezuschusst werden. In Metropolen wie der südchinesischen Stadt Shenzhen finden Start-ups mit Hardware-Ambitionen zudem eine hohe Fabrikdichte und gut ausgebaute Logistiknetzwerke. Prototypen können dort günstig produziert und an den Kunden oder den Investor gebracht werden. Nationale und internationale Wagniskapital-Investoren befeuern Chinas Start-up-Boom weiter.

Chinas Regierung hat seit Anfang 2015 eine Reihe von Maßnahmen zur Förderung der Start-up-Industrie auf den Weg gebracht. Im Mai 2017 richtete sie einen mit umgerechnet 2,6 Milliarden US-Dollar ausgestatteten Wagniskapital-Fonds ein. Damit sollen in erster Linie Start-ups im Hardware-Bereich unterstützt werden. Noch mehr Geld will die chinesische Führung in den Sektor locken, indem sie verstärkt Börsengänge von IT-Start-ups im Inland unterstützt und Restriktionen für ausländische Investitionen in den Bereich lockert. Insbesondere E-Commerce-Unternehmen sollen Pekings Ankündigungen zufolge von vereinfachten Registrierungsvorschriften und Steuererleichterungen profitieren können.

Talentmangel. Fragt man chinesische Start-up-Unternehmer nach der größten Herausforderung für Innovation, antworten sie mehrheitlich: der Mangel an gut qualifizierten Mitarbeitern. Im Bereich privater und staatlicher Finanzierung kann China durch die straffe politische Steuerung von oben schnell Fortschritte erzielen. Das Problem der mangelnden Talente wiegt schwerer: Es geht nicht – so jüngste Umfragen der chinesischen IT-Plattformen iResearch und Changyebang – um fehlendes Fachwissen, sondern vor allem um „Out of the box"-Denken und die Entwicklung kreativer Marketingstrategien. Dazu bräuchte China nicht nur mehr Start-up-bezogene Kurse, sondern ein offenes, pluralistisches Bildungssystem, das auch abweichende Meinungen fördert. Die Vorstöße der Regierung, westliche Lehrbücher an Universitäten zu verbieten und Forscher durch das Verbot ausländischer VPN-Verbindungen von wichtigem globalem Wissensaustausch abzuschneiden, sprechen derzeit jedoch eine andere Sprache.

Herausforderung. Chinas junge IT-Unternehmer stört dies alles wenig, solange sie zwischen Niederlassungen in Silicon Valley, Europa und China frei hin- und herreisen, ihre Mobiltelefone überall benutzen und Daten in den Clouds ausländischer Anbieter lagern können. Nur selten kritisieren sie die Abschottungspolitik Pekings. Sie arrangieren sich, wo es notwendig und gewinnfördernd ist. Ansonsten ziehen es viele von ihnen vor, die Politik einfach zu ignorieren und sich ihre eigene Welt aufzubauen. Das ist vielleicht die größte Herausforderung für die chinesische Regierung, was die angestrebte staatliche Lenkung der digitalen Innovation angeht. Sie erreicht die smarten Gründer mit ihren kollektivistischen Beschwörungen von nationaler Cybersicherheit und „westlicher Infiltration" kaum. Was die Start-up-Unternehmer mit der Digitalisierung verbinden, ist vor allem, genauso reich zu werden wie der Alibaba-Gründer Jack Ma. ⊡

Dr. Kristin Shi-Kupfer leitet bei MERICS den Forschungsbereich Politik, Gesellschaft und Medien. Zuvor war sie wissenschaftliche Mitarbeiterin am Institut für Sinologie der Freiburger Albert-Ludwigs-Uni. Seit 2017 gehört sie zur Expertengruppe der deutsch-chinesischen Plattform Innovation des Bundesministeriums für Bildung und Forschung.

Fotos: feelphoto/sacilad – Shutterstock, merics/Jan Siefke

Digitalisierung im Gesundheitswesen

Zielgerichtete Arbeit an E-Health und der dafür notwendigen Gesetzgebung in China.

Chenchao Liu

Laura Nelson Carney, erfahrene Asia-Pacific-Healthcare-Analystin bei Bernstein Research, bringt es auf den Punkt: „Es ist fair zu sagen, dass die chinesischen Technologieunternehmen im Gegensatz zu den USA sich im Gesundheitsbereich engagieren und aktiv im Gesundheitswesen tätig sind. In den Vereinigten Staaten machen das dagegen nur einige und andere nicht."

Das Gesundheitswesen im Reich der Mitte erlebt gerade eine epochale Zäsur durch die enorme Geschwindigkeit der Digitalisierung und Novellierung zahlreicher Gesetzgebungen und Verordnungen.

China muss diversen Herausforderungen trotzen. In China sind die Krankenhäuser überlastet, und die Arbeitsbelastung der Ärzte ist außergewöhnlich hoch. Es gibt nur etwa 1,5 Ärzte pro 1.000 Personen. Die chinesische Regierung hat als Ziel gesetzt, dass das Land die führende Position in K.I. bis 2030 (13th Five Year Plan of PRC) erreichen soll. Daher fördert die Regierung den entsprechenden technologischen Schub.

Große Internet-Giganten wie Alibaba und Tencent haben die Gesundheitsfürsorge schon vor Jahren zu einem wichtigen Teil ihrer strategischen Agenda gemacht. Dienstleistungen wie medizinische Online-Beratung und Drogenverfolgungssysteme wurden bereits getestet. Diese beiden Technologie-Titanen dominieren die chinesischen E-Commerce-Sektoren. Ihre jüngsten Fortschritte ermöglichen es den Ärzten, effizient mithilfe von Diagnosewerkzeugen zu arbeiten.

Konsultation online. Alibaba hat bereits 2014 den zukünftigen Krankenhausplan vorgestellt, der die Arbeit der Ärzte effizienter machen soll. Im Wesentlichen ermöglicht er es den Ärzten, Patienten online zu konsultieren und dafür zu sorgen, dass die Patienten Medikamente online bestellen können. Dabei wird darauf geachtet, nicht nur den Schutz der Privatsphäre von Patienten zu verbessern und zu regulieren. Das gilt auch für den Verkauf von rezeptfreien Medikamenten. Daher wurde der Verkauf von OTC-Medikamenten auf Alibabas E-Commerce-Website von chinesischen Aufsichtsbehörden ausgesetzt.

Insgesamt beschäftigen sich mehr als 130 chinesische Unternehmen mit K.I. im Gesundheitswesen. So jedenfalls verdeutlichen es Zahlen des Pekinger Beratungsunternehmens Yiou Intelligence. Unter ihnen sind nicht nur Marktführer wie Alibaba und Tencent, sondern auch eine Reihe von Start-ups.

Die Firma Yitu arbeitet an der Entwicklung von Software, welche die Identifizierung von frühen Stadien von Lungenkrebs automatisiert. Die Firma beschäftigt sich mit komplexen Herausforderungen bei der Bilderkennung, wie Krebs-Scans. Diese Software würde nicht nur die Arbeitsbelastung überarbeiteter Ärzte verringern. Sie würde gleichzeitig auch den Zugang zu medizinischer Versorgung sicherstellen.

Verbesserung. Laut Yitu-Gründer Chenxi Liu sind die medizinischen Ressourcen in China sehr knapp und ungleich verteilt. Deshalb sind derzeit noch die Spitzenressourcen in den Provinzhauptstädten konzentriert. Mit diesem System wird, wenn es in Krankenhäusern in ländlichen Gegenden verwendet werden kann, die medizinische Versorgung deutlich verbessert werden.

Dunstglocke. Smog – wie hier in Schanghai – kann Krebs auslösen. K.I. hilft bei der Früherkennung.

Fotos: Hung Chung Chih/Magic mine/PR Image Factory – Shutterstock

Digital-Medizin. Modernste Technik ermöglicht es Medizinern, auch online effizient zu arbeiten.

Alibaba und Tencent haben die Gesundheitsfürsorge schon vor Jahren zu einem wichtigen Teil ihrer Agenda gemacht.

Auch in China haben der Schutz persönlicher Daten, die Rechte an geistigem Eigentum und der globale Fluss von Menschen und Internet-Technologien die ambivalente Entwicklung von E-Health, die aktuellen nationalen Gesetze und Vorschriften sowie regulatorische Systeme infrage gestellt.

Die gegenwärtige Situation in China führt erstmals das Konzept der „persönlichen biometrischen Information" in die Gesetzgebung ein. Im Juni 2015 verabschiedete der Ständige Ausschuss des Nationalen Volkskongresses dazu das „Netzsicherheitsgesetz der Volksrepublik China (Entwurf)". Das Konzept der persönlichen biometrischen Informationen wurde zuerst in die Definition der persönlichen Informationen aufgenommen. Dies bedeutet, dass der Gesetzgeber →

begonnen hat, auf die Merkmale der medizinischen und Gesundheitsinformationen zu achten. Durch die entsprechende Gesetzgebung sollen allmählich die persönliche Informationserfassung, -nutzung und -speicherung von E-Health geregelt werden.

Die Gesundheitsinformationen der Bürger dürfen nicht auf Servern im Ausland gespeichert werden. Man darf ausländische Server auch nicht beauftragen oder ausleihen. Grundsätzlich scheint die Entwicklung von E-Health gemeinsames Ziel der ganzen Welt zu sein, um durch die Digitalisierung das Gesundheitsmanagement und die medizinische Betreuung insgesamt zu verbessern. Aber auch in China sieht man es in den nächsten Jahren als einen Mittelpunkt der Arbeit an, persönliche und die nationale Informationssicherheit zu verbessern. Nur dann lässt sich ein ausgewogenes Gleichgewicht bei der Aufgabe E-Health erreichen.

Bürgerrechte. Laut dem US-amerikanischen Marktforschungsunternehmen Grand View Research (2016) wird der globale E-Health-Markt bis 2022 voraussichtlich 308 Milliarden US-Dollar erreichen. Da mehr und mehr Unternehmen E-Health als ihr Hauptgeschäft ansehen, ist Hightech-Technologie in den Fokus von E-Health geraten. Deshalb treten auch immer häufiger Fragen im Zusammenhang mit dem Recht an geistigem Eigentum auf.

Ob die Rechte des geistigen Eigentums in den Geltungsbereich des Zivil- und Handelsrechts fallen, war in der akademischen Gemeinschaft schon immer ein Thema. Einige Wissenschaftler sind der Ansicht, dass das Recht des geistigen Eigentums ein wichtiger Teil des Zivilrechts ist, während andere der Meinung sind, dass das Recht auf geistiges Eigentum bestimmten Beschränkungen unterliegt. Mit dem Aufkommen dieser Art von Fragen haben solche Diskussionen mehr und mehr Bedeutung erlangt, insbesondere die Forschung zu Bürgerrechten und geistigem Eigentum an „gesundheitsmedizinischen Daten", die an der rapiden Entwicklung von E-Health beteiligt sind. Ein solcher Vorgang ist auch verstärkt in China zu beobachten.

Die drei relevanten grundlegenden Elemente von E-Health sind intelligente Hardware, Software und Daten im Gesundheitswesen. Auf dieser Basis ist man jetzt dabei, ein Netzwerk aufzubauen, das Patienten, medizinische Einrichtungen, Regierungsbehörden, Ein-

Überlastung. **Auch in China ist die personelle Klinik-Situation kritisch.**

richtungen des Gesundheitswesens und des Gesundheitsmanagements verlinkt. Dieser Link umfasst als Kernelemente persönliche Informationen eines Individuums. Dazu zählen Aspekte wie persönliche elektronische Patientenakten, elektronische Gesundheitsakten, Rezepte, Drogenkonsum, allgemeine Berichte, Labor- und Inspektionsberichte oder auch Sport- und medizinische Verbrauchsgewohnheiten.

Fragenbündel. Der Umgang mit den nach dem Datenschutz (in China wird es Gesundheitsdaten genannt) entstandenen Daten, deren Eigentums- und Nutzungsrechte sind ein nachhaltig diskutiertes Thema. An dieser Stelle soll jedoch nicht das Thema des Schutzes personenbezogener Informationen und der nationalen Informationssicherheit behandelt werden. Hier geht es vielmehr um die Bürgerrechte bezüglich der verarbeiteten Daten und die damit verbundenen Fragen des geistigen Eigentums.

Nach dem Zivilrechtssystem umfasst der Besitz an Eigentum vier Aspekte: Besitz, Nutzungsrechte, Einkommensrechte und Verfügungsrechte. Eine Reihe von wichtigen Fragen beherrschen dabei die Diskussionen:

- Wem gehören die Gesundheitsdaten – dem Land, Krankenhäusern, Praxen, einem autorisierten Inkassobüro, einer Informationsverarbeitungsagentur?
- Wem gehört das geistige Eigentum, das Gesundheitsdaten bildet?
- Welche Art von geistigem Eigentum ist geistiges Eigentum an den Daten? Passt es zu den allgemeinen Urheberrechten? (Lou 2016)

Derzeit werden Anwendungen von E-Health-Technologien häufig durch Verarbeitung der Daten in den ursprünglichen Datenbankänderungen durchgeführt. Dazu gehört es auch, einige Inhalte zu entfernen, einige zu ändern und andere hinzuzufügen. Die Daten werden also vielseitig bearbeitet und generalisiert, haben aber immer noch individuelle Merkmale.

Diese individualisierten Merkmale sind nicht länger die Originaldaten, aber es müssen einige Richtungsidentifikationsmerkmale in den Datenmerkmalen vorhanden sein, um bei Bedarf zu den Originaldaten zurückkehren zu können. Gerade deshalb ist der Begriff des Urheberrechts im herkömmlichen, traditionellen Sinn nicht eins zu eins direkt im E-Health-Bereich anzuwenden.

Aufgrund der genannten Probleme ist es schwierig, binnen kurzer Zeit einen umfassenden Konsens zu bilden. Dies wird insbesondere länderübergreifend schwierig, da diverse demografische Faktoren und ein je andersartiger Entwicklungsstand der Technologien für unterschiedliche Positionen sorgen. Deshalb dient der Fortschritt bei der Konkretisierung der Gesetzgebung im Bereich E-Health auch dem verstärkten Wunsch nach einer besseren Harmonisierung der internationalen Regeln und stellt gleichzeitig ein Zeichen der Zukunftsfähigkeit einer Nation in der Digitalisierung dar.

Die gesundheitsbezogenen Daten sind persönliche und sensitive Informationen eines Individuums, zu deren Schutz der Staat samt allen Institutionen verpflichtet ist. Diese persönlichen Daten sollten ausschließlich dazu dienen, Menschen die Vorzüge und Funktionalitäten von E-Health mithilfe dieser Daten uneingeschränkt zur Verfügung zu stellen.

China hat mit der Initiative Healthy China 2030 ambitionierte Ziele für die 1,4 Milliarden Menschen gesetzt. Es bleibt offen, wie stringent und nachhaltig die Maßnahmen und Reformen eine dauerhafte Verbesserung der nationalen Gesundheitsversorgung herbeiführen werden. Digitalisierung wird dabei eine unerlässliche Rolle spielen, wobei es mit Spannung zu beobachten ist, ob China nicht nur technologisch, sondern auch datenschutzrechtlich ein Vorreiter sein kann.

Chenchao Liu
ist in China geboren, lebt seit 2002 in Deutschland. Er ist Gründer und geschäftsführender Gesellschafter des Beratungsunternehmens Silreal in München und der K.I.-gesteuerten Investitionsplattform DH Bioinvest Ltd. in Hongkong, die innovative Gesundheitsunternehmen mit chinesischen Investoren verbindet. Er berät bei Projekten und Verhandlungen mit strategischen Partnern und regulatorischen Organen.

Fotos: Claudius Hauptmann, PR Image Factory/XiXinXing – Shutterstock

So wirkt Chinas Gesetz für Cybersecurity

Betroffen sind alle. Vor allem ausländische Unternehmen müssen Strategien entwickeln, damit umzugehen.

Florian Kessler, Jost Blöchl

Das chinesische Cybersecurity-Gesetz (CSG), das seit dem 1. Juni 2017 in Kraft ist, trifft Regelungen zu Datenschutz, IT-Sicherheit und Verhalten im Internet. In Deutschland finden sich vergleichbare Inhalte in der Datenschutzgrundverordnung (DSGVO), dem IT-Sicherheitsgesetz, den Regelungen zum Äußerungsrecht oder dem Netzwerkdurchsetzungsgesetz. Die chinesische Variante unterscheidet sich jedoch in der Anwendung in etlichen Punkten. Grund hierfür ist eine grundsätzlich andere Ausrichtung. Argumentieren europäische Gesetzgeber primär mit dem Schutz von Persönlichkeitsrechten ihrer Bürger, stehen in China die Erhaltung der „Souveränität über den Cyberspace" und der nationalen Sicherheit im Vordergrund.

Das CSG ist Teil einer Gesamtstrategie zum Aufbau eines digitalen Chinas. An seiner Umsetzung sind diverse Behörden und Institutionen beteiligt, die, teilweise mit Rechtssetzungskompetenz ausgestattet, weitere Vorschriften erlassen. Dies sind Gesetze, Verordnungen oder nationale Standards, die die im CSG nur grob umrissenen Pflichten konkretisieren. Die Titel von circa 300 nationalen Standards, die sich mit IT-Sicherheit und Datenschutz befassen, zeigen, wohin China will: Cloud Computing, Big Data, Internet of Things, industrielle Kontrollsysteme oder Smart City sind nur einige Beispiele für die geplante umfassende Regulierung des digitalen Raums. Viele der Vorschriften befinden sich noch im Entwurfsstadium. Voraussichtlich wird ein Großteil der Vorschriften bis Ende 2018 finalisiert.

Zwingendes Thema: Das CSG gilt für natürliche und juristische Personen, die im Gebiet Chinas Informationen erheben, verarbeiten oder verbreiten. Betroffen sind alle ausländischen Unternehmen mit Niederlassungen in China, aber auch ausländische Unternehmen, die sich zum Beispiel mit ihrer Webseite an chinesische Kunden wenden. Diesen droht bei Verstößen die Blockierung ihrer Angebote in China.

Schwellenwerte für die Anwendbarkeit des Gesetzes, z.B. nach Anzahl der Mitarbeiter oder nach Umfang der Datenverarbeitung, gibt es nicht. Die zu erfüllenden Pflichten variieren aber in Abhängigkeit von der rechtlichen Einordnung als Betroffener nach dem CSG und nach dem Umfang der Datenverarbeitung.

Umsetzungsfokus. Die ersten Anwendungsfälle des neuen Gesetzes be-

Kabelsalat. Vielfalt ohne Kontrolle ist Chinas Behörden suspekt. Das Cybersecurity-Gesetz dient deshalb angeblich auch der nationalen Sicherheit.

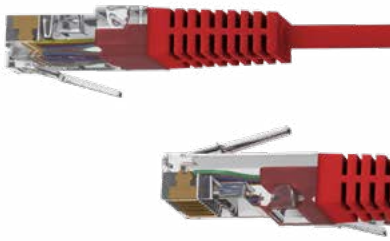
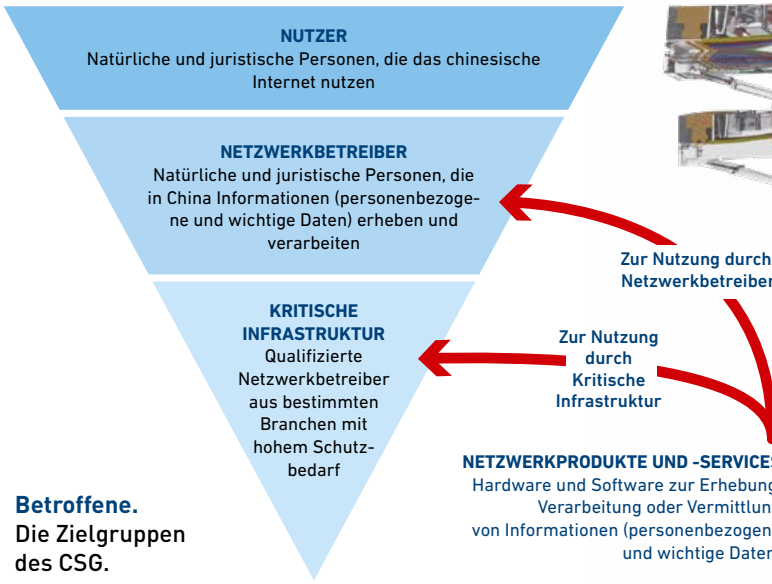


Foto: cherezoff – Shutterstock



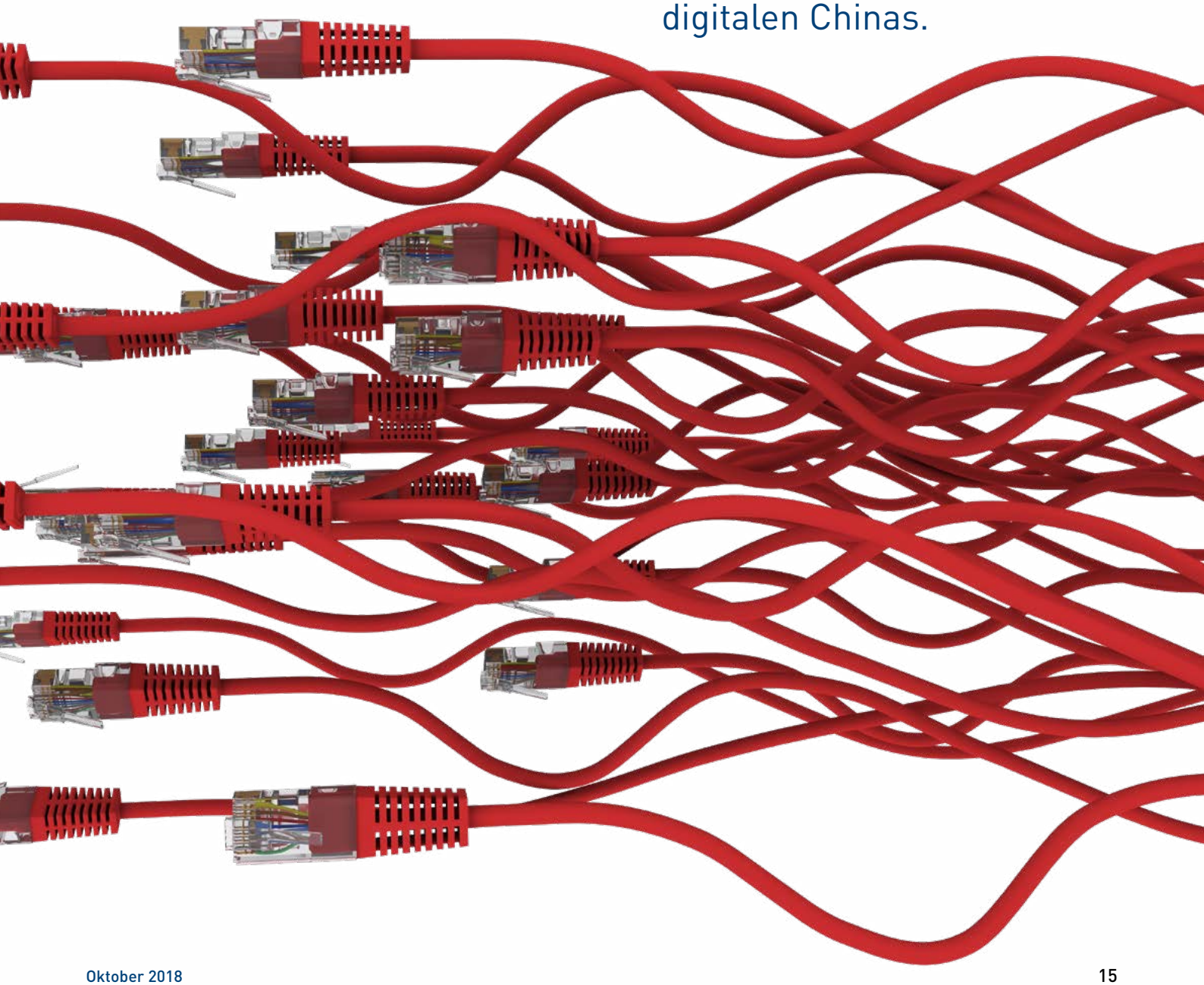
Betroffene. Die Zielgruppen des CSG.

treffen die Steuerung des Verhaltens der Unternehmen und Bürger im Internet und spiegeln damit das chinesische Primat der Erhaltung der Souveränität über den Cyberspace wider. Behörden prüften Webseiten und Social-Media-Kanäle auf die Einhaltung „sozialistischer Werte" und verlangten die Löschung von Inhalten, z.B. Klatschgeschichten oder politisch nicht gewollten Inhalten. Internationale Aufmerksamkeit erlangte der Fall einer Hotelkette, deren Webseite in China für eine Woche gesperrt wurde, weil sie Tibet und Taiwan in einem Auswahlmenü als eigenständige Kategorien aufgeführt hatte.

Weitere Maßnahmen erfolgten zum Datenschutz, z.B. bei der Unterbindung des illegalen Datenhandels. Nach aktuellem Stand werden zukünftig die Polizeibehörden die Aufsicht über die Durchsetzung des CSG führen und nicht unabhängige Datenschutzbehörden. Gründe hierfür sind der gesetzgeberische Fokus des CSG auf die Erhaltung der nationalen Sicherheit sowie die enge Verknüpfung von Datenschutz und Strafrecht. Fälle von Identitätsdiebstahl und Online-Betrug sind ein wachsendes Problem in China, welches die Behörden in den Begriff bekommen wollen.

Beim Datenschutz ergeben sich Parallelen und Besonderheiten im Vergleich zur ➔

Das CSG ist Teil einer Gesamtstrategie zum Aufbau eines digitalen Chinas.



Erfassung. Egal welche Daten: Alles ist fest im Visier.

➜ DSGVO. Das CSG erfasst personenbezogene Daten, die ähnlich der DSGVO nach dem Merkmal der Identifizierbarkeit einer natürlichen Person bestimmt werden. Daneben werden mit Verweis auf die nationale Sicherheit, die wirtschaftliche Entwicklung Chinas und öffentliche Interessen auch „wichtige" Daten vom CSG erfasst. Welche Daten hierunter genau fallen, ist noch nicht geklärt. Ein aktueller Entwurf bezeichnet Daten aus insgesamt 27 Kategorien als wichtig.

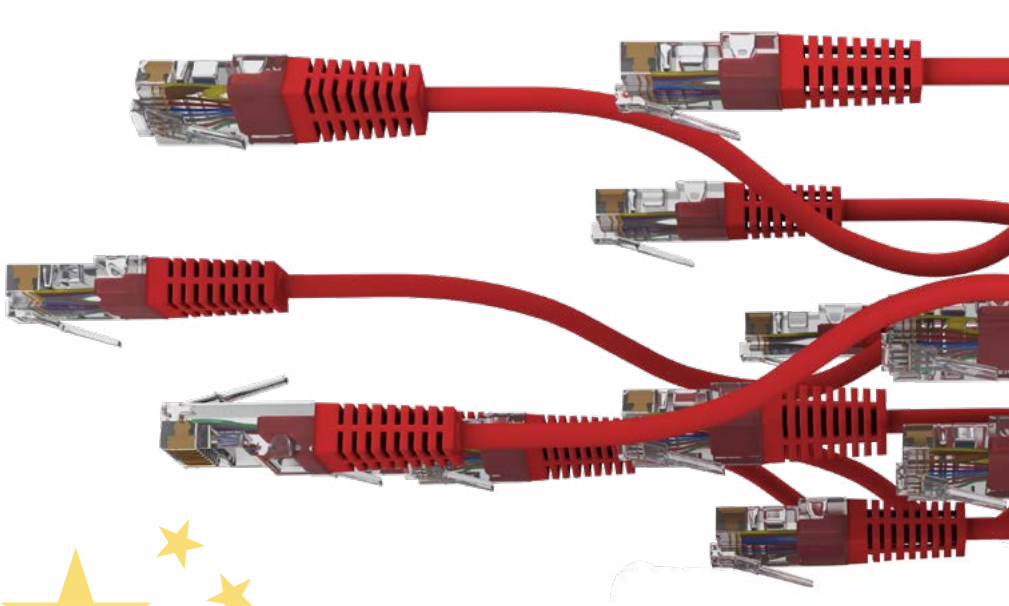
Die Pflichten für den Umgang mit personenbezogenen und wichtigen Daten sind aktuell weitestgehend einheitlich gestaltet. Für die Verarbeitung personenbezogener Daten gelten einige zusätzliche Pflichten. Bei deren Umsetzung können europäische Unternehmen in vielen Fällen auf Vorarbeiten im Rahmen der DSGVO zurückgreifen und müssen diese häufig nur geringfügig an die chinesischen Besonderheiten anpassen. Pflichten wie die Aufzeichnung von Verarbeitungsprozessen, Risikoabschätzungen, ein grundsätzliches Einwilligungserfordernis, die Wahrung von Auskunftsrechten, Berichtigungs- und Löschungsansprüchen oder das Vorhalten einer Datenschutzerklärung finden sich parallel in der DSGVO und den chinesischen Regeln.

Eine große Sorge für ausländische Unternehmen ist die im Raum stehende lokale Speicherpflicht in China. Diese laut CSG nur für Betreiber Kritischer Infrastrukturen geltende Pflicht wurde in einem Entwurf einer Umsetzungsvorschrift auf alle Netzwerkbetreiber erweitert. Bleibt es bei dieser Erweiterung, müssten ausländische Unternehmen ihre IT-Infrastruktur massiv anpassen, z.B. die Wahl von Cloud-Services oder zentral aus dem Ausland betriebene ERP-Systeme oder SAP-Anwendungen. Vor einem Datentransfer in Drittländer werden Unternehmen nach dem Entwurf voraussichtlich eine interne Sicherheitsüberprüfung durchführen und bei größeren Datenmengen eine vorherige Genehmigung einholen müssen.

Kollisionsgefahr. Bei Verstößen gegen das CSG drohen Strafen von Geldbußen bis zum Entzug der Geschäftslizenz.

Die Umsetzungspraxis zeigt, dass ausländischen Unternehmen der Umgang mit dem CSG schwerfällt. Gründe hierfür sind die Regelungsflut, fehlendes geschultes Personal oder Abweichungen von geschriebenem Gesetz und Praxis. So schlagen chinesische Internet-Unternehmen wie Alibaba oder Jingdong in der Praxis (offenbar mit Duldung der Aufsichtsbehörden) einen von den hart formulierten Anforderungen eines empfohlenen Standards abweichenden Weg ein und lassen sich z.B. bei der Registrierung auf ihren Plattformen weitreichende Einwilligungen zusichern.

Alibaba. Ein eigener Weg für das Internetunternehmen wird offenbar von den Behörden geduldet.



Für Unternehmen aus dem Technologie-Bereich kann das CSG zu einer erheblichen Einschränkung des Marktzugangs führen. Betroffen sind vor allem Anbieter von Anwendungen für den Bereich Industrie 4.0. Umsetzungsvorschriften stellen klar, dass Netzwerkprodukte z.B. auch Sensorik oder industrielle Kontrollsysteme sind, mit denen Daten erfasst und verarbeitet werden. Der Begriff der wichtigen Daten wird womöglich viele Informationen aus dem Bereich der industriellen Fertigung erfassen.

Diese potenzielle Marktzugangsbeschränkung hat vor allem mit einer Besonderheit nationaler Standards zu tun. Standards werden in der Regel zur Einhaltung empfohlen und nicht als verpflichtend erlassen. Das CSG fordert aber, dass „zwingende Anforderungen relevanter nationaler Standards" einzuhalten sind. Häufig werden empfohlene Standards faktisch verpflichtend, weil die Einhaltung von Aufsichtsbehörden, Prüfstellen oder Vertragspartnern gefordert wird. Betreiber Kritischer Infrastrukturen sind nach dem CSG gezwungen, nur Netzwerkprodukte und -services einzukaufen, für die die Einhaltung relevanter Standards in Sicherheitsüberprüfungen nachgewiesen ist.

Fotos: GDAE2015/cherezoff/testing – Shutterstock

Smart City. Ermöglicht nur eine umfassende Regulierung die Stadt der Zukunft?

Für Unternehmen aus dem Technologie-Bereich kann das CSG zu einer erheblichen Einschränkung des Marktzugangs führen.

Werden Sicherheitsüberprüfungen nicht oder nur zögerlich durchgeführt, z.B. weil es keine Umsetzungsstrategie gibt, droht der Verlust zukünftiger Aufträge. Vor Kurzem warnte ein amerikanischer Thinktank, dass China eine verstärkte Anwendung der Cybersecurity-Standards als weiteres Mittel im Handelsstreit einsetzen und so für eine Marktabschottung sorgen könnte.

Weitblick. Die Erfüllung der gesetzlichen Mindestanforderungen an Datenschutz und IT-Sicherheit wird für alle Unternehmen in China zu einer regelmäßigen Aufgabe werden. Mit Ausnahme der möglichen Pflicht zur Datenspeicherung in China sind die Anforderungen angesichts der Parallelen zur Rechtslage in Europa für die meisten Unternehmen mit verhältnismäßigem Aufwand handelbar.

Schwerwiegend scheinen die langfristigen Auswirkungen für Unternehmen, die technologiebasiert arbeiten. Diese sollten die weitere Entwicklung der Standards verfolgen und sich soweit möglich an der Erstellung beteiligen, z.B. durch Mitarbeit in internationalen Arbeitsgruppen oder durch Kommentierung von Regelungsentwürfen in China. Anlaufstellen sind z.B. die GIZ oder die Europäische Handelskammer in China. Mit Behörden, Prüfstellen und Kunden, vor allem Betreibern Kritischer Infrastrukturen, ist laufend zu kommunizieren, in welchem Umfang die empfohlenen Regelungen der Standards zwingend werden. Der Aufbau von Expertise und die Schaffung erfolgreicher Strategien zum Umgang mit dem CSG und seinen Umsetzungsvorschriften sind für deutsche Unternehmen ein wesentlicher Baustein für Erhalt und Ausbau der Wettbewerbsfähigkeit auf dem chinesischen Markt. ⊡

Dr. Florian Kessler (o.) und Jost Blöchl sind Rechtsanwälte des Pekinger Büros der Kanzlei WZR. Weitere Informationen zum Cybersecurity-Gesetz, den wichtigsten To-Dos für ausländische Unternehmen und zu weiteren Fragen rund um Investitionen in China unter ➜ *www.wzr-china.com*

Charta der digitalen Grundrechte für Europa

Es geht ums Ganze: Der Vorrang des Menschen, seiner Würde, seiner Freiheit und seiner Verantwortung für die Fortentwicklung der digitalen Techniken steht im Fokus.

Friedrich Graf von Westphalen

Unter dem Dach der ZEIT-Stiftung ist kürzlich eine „Charta der Digitalen Grundrechte der Europäischen Union" veröffentlicht worden. Sie enthält grundlegend Neues, um den mannigfachen – und neuartigen – Bedrohungen der Grundrechte durch die Digitalisierung entgegenzuwirken. Doch es sind nicht wenige, die meinen, dazu bestehe gar kein wirklicher Bedarf. Viele sind fest davon überzeugt: Die Bestimmungen der DSGVO reichen aus, den erforderlichen Schutz der Grundrechte des Bürgers im Blick auf seine personenbezogenen Daten abzusichern.

Doch besorgte Stimmen mahnen, und sie warnen mit guten Argumenten, weil sie zu Recht befürchten, der europäische Gesetzgeber habe mit der Verabschiedung der inzwischen in nationales Recht umgesetzten DSGVO „alle Eier in den einen Korb" gelegt, ohne im Ergebnis einen wirklich effektiven Rechtsschutz zugunsten von Freiheit und Privatheit, vor allem im Blick auf das mit der personalen Würde teilkongruente Recht auf „informationelle Selbstbestimmung", zu gewährleisten.

Drei wesentliche Einwände lassen sich gegen die DSGVO ins Feld führen. Man kann – etwas pauschal – auf bekannte Buchtitel verweisen, die mit prägenden und warnenden Worten das Bedrohungsszenario der um sich greifenden Digitalisie- →

Neue Charta.
Ein Weg soll aufgezeigt werden, um Bedrohungen durch Digitalisierung zu begegnen.

WEITERE INFORMATIONEN
→ *digitalcharta.eu*

Signalwirkung.
Ziel ist: alle digitalen Probleme unter der EU-Flagge gemeinsam lösen.

Foto: Marian Weyo – Shutterstock, www.anthonyboyd.graphics, ZEIT-Stiftung


Viele sind fest davon überzeugt: Die Bestimmungen der DSGVO reichen aus, den erforderlichen Schutz der Grundrechte des Bürgers im Blick auf seine personenbezogenen Daten abzusichern.

Marktmacht. Die Großen der Branche scheinen alles fest im Griff zu haben.

→ rung umschreiben, etwa das Buch von Stefan Aust/Thomas Amman, „Digitale Diktatur", oder das Buch der diesjährigen Theodor-Heuss-Preisträgerin, Yvonne Hofstetter, die das „Ende der Demokratie" in Zeiten dominanter Sozialer Medien und sich rasant ausbreitender Künstlicher Intelligenz anbrechen sieht. Man kann auch den von Jakob Augstein kürzlich herausgegebenen Band „reclaim autonomy" als Beleg anführen. Genug.

Irrglaube. Solche Belegstellen ersetzen nicht die juristisch-politische Argumentation. Doch der wohl ganz entscheidende und nachhaltige Beleg gegen die Wirkkraft der DSGVO, ein Bollwerk gegen die bedrohte Freiheit des Bürgers in Zeiten der Digitalisierung zu sein, speist sich aus einem Erfahrungssatz. Er durchzieht das gesamte europarechtlich strukturierte Verbraucherschutzrecht wie ein roter Faden: Es ist der durch nichts belegte Irrglaube des Gesetzgebers, dass mehr oder weniger umfassende Informationen, die dem Verbraucher von Gesetzes wegen vor Abschluss eines Vertrages mitgeteilt werden, seine Wahl- und Entscheidungsfreiheit tatsächlich stärken. Es ist das Bild des „informierten Verbrauchers". Doch dieses Bild als Prototyp des Verbrauchers als des „Menschen im Recht" (Gustav Radbruch) ist ein Zerrbild; es findet keine Korrespondenz in der Alltagswirklichkeit.

Alle Erfahrung besagt: Die Informationen – auch wenn es sich um Vertragsbedingungen handelt – werden vom Verbraucher – mag er gebildet oder ungebildet sein – schlicht nicht gelesen; der rasche „Klick" signalisiert stets die uneingeschränkte Zustimmung des Nutzers. Das nennt man im Ergebnis einen Vertragsabschluss, beruhend auf rechtsgeschäftlich wirksamen Erklärungen. Ohne Einschränkungen gilt dies auch für die „Einwilligung" (Zustimmung) nach Maßgabe der DSGVO. Hinzu tritt auch stets der Bequemlichkeitsfaktor, dem kaum ein Verbraucher widersteht: Die Überlassung der personenbezogenen Daten – Zweckangabe hin oder her – erfolgt ja zudem „for free", und die dann „unentgeltlich" zu nutzenden „Dienste" von Google, Amazon oder Facebook verheißen ja ein „besseres" Leben mit Freunden, versteht sich.

Spezieller Einwand: Eine datenschutzrechtliche Zustimmung des Nutzers ist nach Art. 6 Abs. 1 lit a DS-GVO gesetzlich nicht gefordert, wenn und soweit „die Verarbeitung personenbezogener Daten für die Erfüllung des Vertragszwecks erforderlich" ist. Der Vertragsabschluss – „for free" – regiert also, und der Vertragszweck heiligt die Mittel der Werbeplattformen. Sie erhalten die personenbezogenen Daten des Nutzers, und das Resultat ist: die Manipulation des Nutzers bis zu seiner dauerhaften Gefangennahme in der „Filterblase"; die Daten der Nutzer – vor allem die der Wohlhabenden – sind eben das Gold des Internet-Kapitalismus. Im Hintergrund steht inzwischen die harte Frage, ob denn die verhaltenssteuernden Algorithmen uns nicht mehr und nachhaltiger steuern als das Recht.

Ein Drittes, wohl das Wichtigste: Unser liberales Grundrechtsverständnis ist davon geprägt, dass die Grundrechte Abwehrrechte gegenüber dem (nationalen) Staat sind, die der Bürger zum Schutz von Würde und Freiheit in Stellung bringen kann. Doch die Bedrohungen des digitalen Zeitalters gehen von Internet-Giganten aus, also von Unternehmen; dem Staat bleibt das zweifelhafte Privileg der öffentlich gesteuerten Überwachung. Rechtlich gewertet vollziehen sich diese „Angriffe" von Big Data aber auf horizontaler Ebene, nämlich innerhalb der Privatrechtsordnung.

Rechtsbefehle. Doch die im Silicon Valley beheimateten Internet-Konzerne sind jedenfalls faktisch weitestgehend extraterritorial. Ihre unglaubliche wirtschaftliche Macht wirft inzwischen die schwerwiegende Frage auf, ob und wie lange noch ein Rechtsstaat es zulassen darf, dass – Beispiel: Besteuerung – sich innerhalb seines Territoriums Mächte entfalten, die er nicht mehr uneingeschränkt beherrschen kann. Das ist qualitativ wesentlich mehr als die oft vernommene Frage, ob denn die Politik sich noch gegenüber den Großen der Wirtschaft durchsetzen kann, ob sie noch den politischen Primat in Anspruch nehmen und ihre Rechtsbefehle auch mit Anspruch auf Autorität durchsetzen kann.

Gerade unter diesem Blickwinkel ist es von ganz entscheidender Bedeutung, dass jetzt die Digitale Grundrechtscharta in Artikel 23 Absatz 3 bestimmt, dass die

Fotos: Brian A Jackson/DenisProduction.com/Mykola Komarovskyy/ymgerman– Shutterstock, Frank Bluemler

Der Vorrang des Menschen, seiner Würde, seiner Freiheit und seiner alleinigen Verantwortung für die Fortentwicklung der digitalen Techniken steht im Fokus.

„Rechte und Pflichten" aus dieser Charta „für alle Unternehmen" gelten, „die auf dem Gebiet der EU tätig sind". Der Jurist nennt die damit angesprochene Rechtsfigur eine „Drittwirkung", also die Verankerung des Durchsetzungsanspruchs der digitalen Grundrechte nicht nur gegenüber dem Staat, sondern auch gegenüber „Unternehmen". Diese – weiter gehende – Rechtswirkung der Grundrechte hinein ins Privatrecht ist dem deutschen Verfassungsrecht durchaus (in Grenzen) vertraut. Sie hat aber innerhalb der Grundrechtscharta der EU überhaupt keinen Platz. Denn Artikel 51 der Grundrechtscharta der EU stellt unmissverständlich klar, dass „diese Charta für die Organe, Einrichtungen und sonstigen Stellen der Union" gilt und eben auch nur „für die Mitgliedstaaten ausschließlich bei der Durchführung des Unionsrechts".

Genau dieses Defizit im Grundrechtsschutz des Bürgers wird und soll durch die Digitale Grundrechtscharta beseitigt werden. Das ist nicht nur auf der Ebene des politischen Diskurses, sondern auch auf der Ebene der rechtspolitischen Debatte in Europa ein immenser Fortschritt. Ein Denkanstoß, eine Handlungsanleitung. Sie ist vor allem unter dem Blickwinkel bedeutsam, dass ja die vielfältigen Herausforderungen der Digitalisierung – auch im Blick auf ihr vorhandenes und oft unterschätztes Bedrohungspotenzial – nur im Rahmen eines noch mühsam zu schaffenden europäischen Rechts bewältigt werden können. Das wird viele Jahre in Anspruch nehmen.

Datenhaufen. Daher springt auch die Neuformulierung des Würdeanspruchs in Artikel 1 Absatz 2 der Digitalen Grundrechtscharta ins Auge: „Neue Gefährdungen der Menschenwürde ergeben sich im digitalen Zeitalter insbesondere durch Big Data, künstliche Intelligenz, Vorhersage und Steuerung menschlichen Verhaltens, Massenüberwachung, Einsatz von Algorithmen, Robotik und Mensch-Maschine-Verschmelzung sowie Machtkonzentration bei privaten Unternehmen." Es geht also um nicht mehr, aber auch um nicht weniger; es geht ums Ganze: Der Vorrang des Menschen, seiner Würde, seiner Freiheit und seiner alleinigen Verantwortung für die Fortentwicklung der digitalen Techniken steht im Fokus. Nach unserem Rechtsverständnis ist es ausgeschlossen, den Menschen als Person mit Leib und Seele nur als einen steuerbaren „Datenhaufen" zu behandeln. Das kybernetische Menschenbild der Wissenschaft, das den Menschen lediglich als einen USB-Stick in ihre planende Programmierung nimmt und mit Beschlag belegt, ist nicht das Menschenbild des europäischen Rechts. Und es darf daher auch nicht zu einer mathematisch determinierten Größe pervertiert werden. Dagegen ist fundamentaler Widerstand angesagt.

Notwendigerweise sind daher auch die weiteren Forderungen der Digitalen Grundrechtscharta – außerhalb des rein Appellativen, sondern mit verpflichtendem Bezug zur gesellschaftlichen Gestaltung Europas – in den Blick zu nehmen: „Ethisch-normative Entscheidungen können nur vom Menschen getroffen werden." (Artikel 8 Absatz 1) Und im Blick auf die weithin nicht voll beherrschbaren Risiken der Künstlichen Intelligenz steht zu lesen: „Für die Handlungen selbstlernender Maschinen und die daraus resultierenden Folgen muss immer eine natürliche oder juristische Person Verantwortung tragen." Dann schließlich auch dieser Programmsatz gegen die Wirkmacht der Algorithmen: „Jeder hat das Recht, nicht Objekt von automatisierten Entscheidungen von erheblicher Bedeutung für die Lebensführung zu sein" (Artikel 7 Absatz 1).

Wirrwarr. Immer nur der Mensch sollte entscheiden, wohin der Weg geht.

Prof. Dr. Friedrich Graf von Westphalen leitet den Ausschuss „Europäisches Privatrecht" beim Rat der Europäischen Anwälte in Brüssel, ist Mitglied des European Law Institute Wien.

Digitale Agenda oder digitale Strategie?

In den letzten Jahren wurde einiges geschafft. Sichtbar geworden ist vor allem jedoch ein strategisches Defizit. Worauf es jetzt ankommt.

Göttrik Wewer

Die intensiv diskutierte Frage, ob das Thema Digitalisierung so bedeutsam ist, dass es in einem eigenen Ministerium gebündelt werden sollte, oder aber in jedem Ressort bearbeitet werden muss, da es alle Politikfelder umpflügt, ist vorerst entschieden: Mit der Berufung einer „Staatsministerin für Digitalisierung" im Kanzleramt hat die Bundeskanzlerin einem Digitalministerium eine Absage erteilt und das Thema zugleich zur „Chefsache" gemacht. Wenn auf diesem Feld in den nächsten Jahren zu wenig passiert, dann fällt das direkt auf die Regierungschefin zurück.

Die Staatsministerin für Digitalisierung, was in anderen Ressorts dem Status eines Parlamentarischen Staatssekretärs entspricht, ist nur eine von drei Staatsministerinnen im Kanzleramt, dessen Chef nicht nur das Haus leitet, sondern noch Bundesminister für besondere Aufgaben ist. Hinzu kommen noch ein Staatsminister als Koordinator für Bürokratieabbau und bessere Rechtsetzung sowie ein (beamteter) Staatssekretär als Beauftragter für die Nachrichtendienste.

Die neue Abteilung 6 (von insgesamt sieben), die sich um „Politische Planung, Innovation und Digitalpolitik, Strategische IT-Steuerung" kümmern soll, befindet sich noch im Aufbau. Vorgesehen sind zwei Gruppen innerhalb dieser Abteilung: eine Planungsgruppe aus drei Referaten, zu der auch das Referat „Wirksam regieren" gehört, und eine „Digitalgruppe" aus fünf Referaten, darunter „Grundsatzfragen der Digitalpolitik", „Digitale Infrastruktur" und „Digitaler Staat", von denen die meisten Leitungen aktuell (27.08.18) noch nicht besetzt sind. Die Leitung der neuen Abteilung ist einer langjährigen Mitarbeiterin der Kanzlerin übertragen worden, die früher den Stab „Politische Planung, Grundsatzfragen, Sonderaufgaben" und das Referat „Medienberatung" geleitet hat.

Verschmelzung. Im Vergleich zu den großen Ressorts, die sich ebenfalls um das Megathema kümmern, wirkt die Staatsministerin unzureichend ausgestattet: Ohne gut dotierte Förderprogramme und mit nur einer Handvoll Referaten lässt sich nicht viel bewegen. Das erste Jahr der Wahlperiode ist schon vorbei; die Abteilung wächst erst langsam.

Die Frage, was die Staatsministerin im Kanzleramt überhaupt bewirken kann, stellt sich auch deshalb, weil man nicht

Flatterhaft. Der Weg vom Pixelfähnchen zur großen digitalen Bundesflagge scheint noch nicht gefunden.

nur dort, sondern auch im Bundesministerium des Innern neue Abteilungen gegründet hat: nicht nur die für Heimat, sondern auch eine für „Digitale Gesellschaft, Verwaltungsdigitalisierung und Informationstechnik". Darin sind die früheren Abteilungen für die Modernisierung der Verwaltung und für die Informationstechnik verschmolzen worden, zwischen denen es zahlreiche Schnittstellen gab.

„Wir bündeln Kompetenzen, um den digitalen Wandel zu gestalten", hört man aus dem Haus. Künstliche Intelligenz, Smart (Government) Services, Blockchain, aber auch Hatespeech, digitale Spaltung oder die Übermacht einzelner digitaler Akteure seien Themen, die für gesellschaftliche Herausforderungen ersten Ranges stehen. Gemeinsam mit dem Bundesministerium für Justiz und für Verbraucherschutz habe man die Federführung für die Datenethikkommission der Bundesregierung übernommen; außerdem werde man sich um die Digitalisierung der Verwaltung und des Ehrenamtes kümmern.

Da auch andere Ressorts ähnlich große Projekte und Programme betreiben, bleibt die Frage, was es eigentlich für die Staatsministerin im Kanzleramt noch zu tun gibt, außer Grußworte zu halten.

Fotos: Michael Lucan, Lizenz: CC-BY-SA 3.0 de [CC BY-SA 3.0 de (https://creativecommons.org/licenses/by-sa/3.0/de/deed.en)], from Wikimedia Commons, Top Vector Studio/Vincent Vroom – Shutterstock

Wohin? **Kann Staatsministerin Dorothee Bär entscheidende Ansätze vorgeben?**

Sicher, die Kanzlerin wird sich im Kabinettsausschuss Digitalisierung, dem sie vorsitzt und dem alle Minister angehören, häufig vertreten lassen müssen, weil irgendwo Krisen zu bewältigen sind, und auch der Chef des Kanzleramtes, der durchaus eine Affinität zu diesen Themen hat, dürfte meist mit anderen dringlichen Vorgängen beschäftigt sein. Die Sitzungen des Digitalrates vor- und nachbereiten, der die Regierung beraten soll, muss jemand machen, dies füllt aber niemanden aus, der politisch gestalten möchte. Was also dann?

Eckpunkte. In den letzten Jahren ist einiges geschafft, aber auch manches verpasst worden. Sichtbar geworden ist vor allem ein strategisches Defizit. Die „Digitale Agenda 2013–2017" bestand im Grunde aus Projekten, die von den Ressorts vermutlich ohnehin betrieben worden wären, alle für sich sinnvoll, aber insgesamt ohne klare Prioritäten und ohne eine Richtung vorzugeben. Dass hier ein Defizit besteht, scheint man im Kanzleramt verstanden zu haben: Die Vorschläge aus den Ressorts, die über den Sommer gesammelt wurden, sollen bis zum Herbst zu einer gemeinsamen Strategie verdichtet werden, hieß es nach der ersten Sitzung des Kabinettsausschusses Digitalisierung am 27. Juni. Künstliche Intelligenz, Blockchain und die Zukunft der Arbeit seien wichtige Themen, zu denen man sich strategisch besser aufstellen wolle.

Im Juli hat das Kabinett Eckpunkte für eine Strategie Künstliche Intelligenz beschlossen, die jetzt federführend von den Ministerien für Wirtschaft und Energie, für Bildung und Forschung sowie für Arbeit und Soziales ausgebaut werden sollen. Ende des Jahres soll die Strategie auf dem Digital-Gipfel in Nürnberg öffentlich präsentiert werden. Deutschland soll zum „weltweit führenden Standort" auf diesem Feld werden, „Artificial Intelligence (AI) made in Germany" zum weltweit anerkannten Gütesiegel.

Wenn die Staatsministerin im Kanzleramt sich darauf konzentriert, die strategischen Defizite abzubauen, die zuletzt immer deutlicher wurden, dann kann sie womöglich auch mit bescheidenen Ressourcen relativ viel bewegen. Keine neue „Agenda" mit einzelnen Projekten abarbeiten, mitunter auch noch schlecht aufeinander abgestimmt, sondern die Digitalpolitik der Bundesregierung strategisch neu ausrichten, darauf käme es an. Wenn auch das Innenministerium seine Digitalstrategie für die Verwaltung überdenkt, wäre das eine sinnvolle Ergänzung.

Eine Verwaltung, die ihre Dienste auch online anbietet, ist noch lange keine digitale Verwaltung. Das wäre sie erst, wenn sie systematisch die Daten erhebt, die sie braucht, um ihre Aufgaben besser erledigen und das öffentliche Leben intelligenter managen zu können. Die digitale Verwaltung ist eine datengesteuerte, manche sagen: eine datengetriebene Verwaltung („data-driven").

Hoffnungswunsch. Ohne eine klare Strategie, wie man dorthin kommt, die Möglichkeiten des digitalen Zeitalters auch selbst zu nutzen, droht die Verwaltung noch weiter hinter Wirtschaft und Gesellschaft zurückzufallen, als sie das heute schon ist. Bleibt zu hoffen, dass man das im Kanzleramt begriffen hat. ⊡

Dr. Göttrik Wewer
ist Experte für Electronic Government und Open Government.

IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern

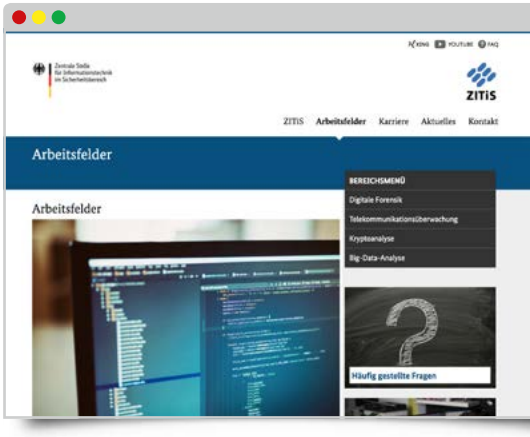
Dringend gefordert: Maßnahmen zum Schutz unserer digitalen Infrastrukturen und privater Kommunikation

Konstantin von Notz

Vor einigen Monaten gelang es Hackern, in das hochgesicherte Netz des Bundes einzudringen und sich darin mindestens ein halbes Jahr unentdeckt zu bewegen. Dabei wurde das Netzwerk des Bundes von der Bundesregierung nach einem ähnlich verheerenden Angriff auf den Deutschen Bundestag als eines der sichersten Netze überhaupt gepriesen. Der Angriff kann nicht als singuläres Ereignis betrachtet werden. Er reiht sich in eine ganze Kette vergleichbarer Attacken auf digitale Infrastrukturen und IT-Systeme ein, die von Staaten, öffentlichen Einrichtungen, Unternehmen und Privatpersonen genutzt werden. Deutlich wurde erneut: Insgesamt steht es schlecht um die IT-Sicherheit in Deutschland.

Seit Jahren weisen wir darauf hin, dass in unserer zunehmend vernetzten Welt auch die Bundesregierung in der Pflicht steht, einen hohen Schutz von Netzen, IT-Systemen und privater Kommunikation zu garantieren. Eine solche Schutzverpflichtung lässt sich, darauf haben Verfassungsrechtler wiederholt hingewiesen, direkt aus unserem Grundgesetz ableiten.

Dennoch wird die Bundesregierung dieser Schutzverantwortung bis heute nicht gerecht. Dies ist insofern auch vollkommen unverständlich, als dass Vertrauen in gute IT-Sicherheit und die Privatheit von Kommunikation nicht nur die Voraussetzung für die gemeinwohlorientierte Gestaltung der Digitalisierung, sondern auch für die Akzeptanz in neue digitale Angebote und E-Government ist.



ZITIS. Eine umstrittene Einrichtung ohne klare Abgrenzung zu anderen Vorhaben.

Maßnahmen unzureichend. Die bisherigen Maßnahmen der Bundesregierung zum Schutz der IT-Sicherheit sind absolut unzureichend: Erst wurde die IT-Sicherheit über Jahre der Selbstregulierung der Wirtschaft überlassen. Dann wurde von der letzten großen Koalition ein IT-Sicherheitsgesetz verabschiedet, das seinen Namen kaum verdient. Insgesamt bleibt die IT-Sicherheitspolitik der Bundesregierung höchst widersprüchlich. Um nur ein Beispiel zu nennen: Ob man Verschlüsselung nun politisch unterstützen oder mit neuen Behörden wie ZITIS lieber flächendeckend brechen will, man scheint es selbst nicht genau zu wissen.

Im Bereich der IT-Sicherheit irrlichtert die Bundesregierung orientierungslos durch den digitalen Raum. Erst vor wenigen Wochen musste sie erneut einräumen, dass sie auf zentrale, verfassungsrechtlich heikle Fragen auch weiterhin keine Antworten hat. Dies gilt u.a. für weiterhin hochumstrittene „Hackbacks", also offensive Gegenschläge, aber auch den staatlichen Umgang mit IT-Sicherheitslücken.

Rechtliche Klarstellungen sind seit Jahren überfällig, werden aber bewusst verschleppt. Dies ist schlecht für die Rechtssicherheit von Unternehmen und die Akzeptanz digitaler Innovationen. Zudem gefährdet es Grundrechte und bestärkt Staaten wie China, denen man so ganz gewiss kein Entgegenkommen bei gerade gescheiterten, aber weiterhin dringend benötigten neuen Abkommen, beispielsweise zur Ächtung von Cyberwaffen im Rahmen von UN-Verhandlungen, abringen kann.

Militarisierung. Dennoch treiben derzeit vor allem Ursula von der Leyen und Horst Seehofer die Militarisierung des digitalen Raums weiter voran und schaffen gänzlich neue Gefahren. Der Name der neuen „Agentur für Innovationen in der Cybersicherheit" ist reiner Etikettenschwindel. Diese Agentur würde die IT-Sicherheit ganz bestimmt nicht erhöhen, sondern zusätzlich gefährden – und zwar massiv.

Die Pläne für die neue Cyberagentur könnten unausgegorener kaum sein. Was sie eigentlich leisten, auf welcher Rechtsgrundlage sie arbeiten soll oder wie eine Abgrenzung zu – ebenfalls höchst umstrittenen – Einrichtungen wie ZITIS aussehen soll – all das weiß die Bundesregierung scheinbar selbst nicht.

Eine Abstimmung mit anderen Ministerien, beispielsweise dem Auswärtigen Amt, das seit Jahren eine dezidiert andere Politik verfolgt und dessen internationale Bemühungen zur Verbesserung der IT-Sicherheit so massiv torpediert werden, fand scheinbar nicht statt. Aus gutem Grund haben sich auch Abgeordnete aus den regierungstragenden Fraktionen öffentlich gegen die unausgegorenen und die IT-Sicherheit gefährdenden Pläne ausgesprochen. Geholfen hat es nichts.

Knappe Ressourcen. Die Bundesregierung muss endlich umsteuern. Statt die Eskalationsspirale im digitalen Raum weiter zu befördern, muss sie eine echte Kehrtwende im Bereich der IT-Sicherheit vornehmen. Auch vor dem Hintergrund, dass es eine beinahe irrwitzige Annahme ist, ein cyberpolitisches Wettrüsten gegen Staaten wie Nordkorea, China und Russland gewinnen zu können, sollten sich die wenigen zur Verfügung stehenden Ressourcen auf die notwendige Härtung und den Schutz digitaler Infrastrukturen konzentrieren. Die Bundesregierung muss sich gemeinsam mit ihren Verbündeten für neue internationale Regelungen und Kontrollregime engagieren. Genau wie die Ächtung von Antipersonenminen brauchen wir auch die Ächtung bestimmter Praktiken der Cyberkriegsführung und -technologien. Nur das sorgt langfristig für Sicherheit und Freiheit im digitalen Raum.

Offensive Operationen und sogenannte „Hackbacks", der staatliche Ankauf, das Offenhalten und die ➔

Brüchige Sicherheit. Auch der Bundestag wurde gehackt. Deutlichstes Zeichen, dass es einiges zu tun gibt.

Fotos: piick – Shutterstock, www.zitis.bund.de

> Anlasslose Massendatenspeicherungen ohne erwiesenen sicherheitspolitischen Mehrwert und zulasten von Grundrechten sind auch weiterhin abzulehnen.
>
> **Konstantin von Notz**

Fotos: piick – Shutterstock, www.von-notz.de

➔ weitere Nutzung von bislang nicht öffentlich bekannten Sicherheitslücken („Zero-Day-Exploits") sowie Überlegungen einer gesetzlichen Verpflichtung für Unternehmen, Hintertüren in Hard- und Software zu verbauen, sind konsequent abzulehnen. Sicherheitslücken müssen schnellstmöglich im Zusammenspiel staatlicher und privater Akteure geschlossen und der Öffentlichkeit bekannt gemacht werden.

Anlasslose Massendatenspeicherungen ohne erwiesenen sicherheitspolitischen Mehrwert und zulasten von Grundrechten sind auch weiterhin abzulehnen. Zudem brauchen wir, will man an diesen Instrumenten festhalten, endlich zumindest klare Rechtsgrundlagen für den Einsatz von Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung. Diese fehlen bis heute.

Maßnahmenbündel. Der Staat hat für die Vertraulichkeit und Integrität informationstechnischer Systeme zu sorgen und das Grundrecht auf Privatheit der Kommunikation zu wahren und auszubauen. Damit die Bundesregierung dieser weiterhin drängenden Aufgabe endlich tatsächlich nachkommt, haben wir einen umfassenden Katalog mit 25 Maßnahmen zur Erhöhung der IT-Sicherheit vorgelegt.

Wir fordern die Bundesregierung u.a. auf, schnellstmöglich ein neues IT-Sicherheitsgesetz vorzulegen, das seinen Namen tatsächlich verdient, sehr viel breiter ansetzt und Anreize für proaktive Investitionen in gute IT-Sicherheitslösungen schafft. Auch die weiterhin mangelnde Koordinierung und ungeklärte Zuständigkeiten muss die Bundesregierung endlich auflösen.

Weiterhin scheint es notwendig, die Verantwortung für IT-Sicherheit aus dem Bundesinnenministerium herauszulösen. Zu groß sind die Interessenkonflikte, beispielsweise bezüglich des notwendigen Schutzes digitaler Infrastrukturen und privater Kommunikation und der weiterhin extrem hohen Begehrlichkeiten der Sicherheitsbehörden, die ein „going dark" um jeden Preis verhindern wollen. Ein solcher Anspruch ist sicherheitspolitisch eventuell verständlich, aus einer rechts- und demokratiepolitischen Perspektive jedoch abzulehnen. Denn einen solchen Anspruch, in jedweden Kommunikationsvorgang schauen zu können, kennen wir bislang nur aus autoritären und totalitären Staaten wie China. Statt eines auf die Allgemeinheit und die Schwächung der IT-Sicherheit insgesamt abzielenden Ansatzes brauchen wir eine zielgerichtete, polizeiliche Abwehr konkreter Gefahren auf klaren Rechtsgrundlagen. Das ist die Erkenntnis der letzten Jahre.

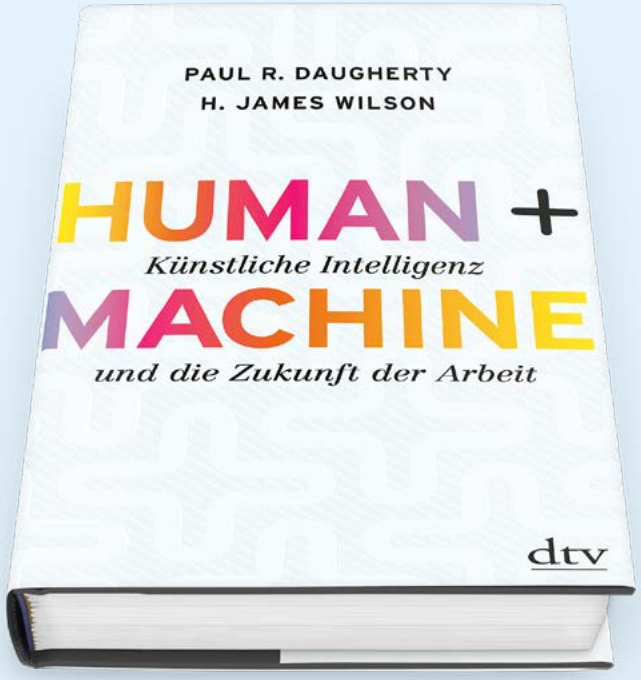
Auch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) ist noch immer dem Innenministerium unterstellt. Wie zuvor die Bundesdatenschutzbeauftragte (BfDI) wollen wir es aus dem Verantwortungsbereich des BMI herauslösen. Nur so kann es eine unabhängige Beratung tatsächlich leisten. Ferner machen wir uns dafür stark, dass die bestehenden Aufsichtsstrukturen sehr viel besser ausgestattet werden.

Unterstützung der Wirtschaft. Einseitige Abhängigkeiten von wenigen IT-Dienstleistern, deren Software nicht überprüfbar ist, muss behoben und der Einsatz und die hohe Qualität von quelloffener Software politisch stärker unterstützt werden. Bei allen E-Government-Angeboten sind beste IT-Sicherheitslösungen auf dem neuesten Stand der Technik, wie zum Beispiel durchgehende Ende-zu-Ende-Verschlüsselungen, zum Standard zu machen. Dabei müssen Datenschutz und IT-Sicherheit zwingend zusammen gedacht werden. Mit Zertifizierungen sollen Anreize geschaffen werden, in gute und sichere IT-Lösungen, insbesondere beim „Internet der Dinge" (IoT), zu investieren. Kleinere und mittlere Unternehmen müssen bei sicherheitstechnischen Herausforderungen durch ein dezentrales und unabhängiges IT-Beratungsnetzwerk unterstützt werden. Haftungsanreize für alle in der IT-Kette verantwortlichen Stellen wollen wir stärken und Anbieter zur Bereitstellung von Sicherheits-Updates verpflichten.

Diese und weitere Maßnahmen zum Schutz unserer digitalen Infrastrukturen und unserer privaten Kommunikation sind überfällig. Die Bundesregierung muss sie endlich umsetzen – zumindest, wenn sie sich nicht weiter vorhalten lassen will, selbst eine Gefahr für die IT-Sicherheit darzustellen, und sie ihre eigenen Sonntagsreden zum notwendigen Grundrechtsschutz im Digitalen ernst nimmt. ⊡

Dr. Konstantin von Notz
ist stellvertretender Fraktionsvorsitzender von Bündnis 90/Die Grünen und netzpolitischer Sprecher seiner Fraktion.

Aktuelle Bücher



Human + Machine

Künstliche Intelligenz und die Zukunft der Arbeit

Paul R. Daugherty, H. James Wilson

Künstliche Intelligenz ist kein Zukunftsszenario, sondern längst mitten in der Gesellschaft angekommen. Höchste Zeit also, sich mit der grundlegenden Transformation unseres Arbeitslebens auseinanderzusetzen. Denn KI, davon sind die Autoren überzeugt, bietet auch eine große Chance, die Arbeit menschlicher und abwechslungsreicher zu gestalten.

dtv, ISBN: 978-3-423-28993-1, 25,00 €

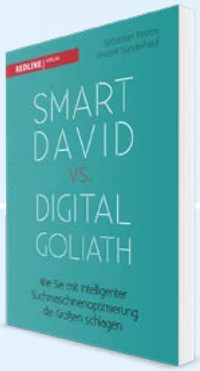
Smartphones als digitale Nahkörpertechnologien

Zur Kybernetisierung des Alltags

Timo Kaerlein

Das Smartphone ist zu einem unentbehrlichen Medium des Selbst- und Weltbezugs geworden. Der Autor beleuchtet neue Aspekte des vermeintlich vertrauten Objekts – darunter etwa die häufig der Sichtbarkeit entzogenen Kontrollinfrastrukturen.

transcript verlag, ISBN: 978-3-8376-4272-8, 34,99 €



Smart David vs Digital Goliath

Wie Sie mit intelligenter Suchmaschinenoptimierung die Großen schlagen

Sebastian Petrov, Vincent Sünderhauf

Findet man beim Googeln die eigene Firma erst auf der dritten Seite? Wie sich das clever ändern lässt, verraten zwei Experten für Suchmaschinenoptimierung. Sie zeigen, wie Suchmaschinen funktionieren.

Redline, ISBN: 978-3-86881-702-7, 19,99 €

Cybersecurity Best Practices

Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden

Michael Bartsch, Stefanie Frey (Hrsg.)

Die Vielzahl der IT-Systeme hat zu hohen Sicherheitsrisiken für Unternehmen und staatliche Einrichtungen geführt. Daher müssen Institutionen Strategien und Lösungen zu ihrem Selbstschutz entwickeln.

Springer Vieweg, ISBN: 978-3-658-21655-9, 49,99 €

Datenschutz im Internet

Rechtshandbuch zu DSGVO und BDSG

Jandt / Steidle (Hrsg.)

Mit dem neuen Datenschutzrecht gelten ab dem 25.5.2018 komplett neue Rechtsgrundlagen auch für die internetspezifischen Datenschutzvorschriften. Dieses Werk behandelt alle datenschutzrechtlichen Aspekte des neuen Rechts. Es wendet sich an Anbieter von Dienstleistungen rund um das Internet, Nutzer und Rechtsberater in Unternehmen und Kanzleien.

Nomos, ISBN: 978-3-8487-4856-3, 89 €

Hinweise zur EU-Datenschutz-Grundverordnung

Seit dem 25. Mai 2018 gilt die neue EU-Datenschutz-Grundverordnung (EU-DSGVO) in Deutschland verbindlich. Das bringt für alle – und natürlich auch für DIVSI – Änderungen mit sich.

Speziell für das DIVSI magazin bitten wir deshalb um Beachtung:

Auch diese Ausgabe 2/2018 haben Sie wie zuvor kostenfrei und ohne weitere Verpflichtung postalisch zugestellt bekommen. Wir nutzen Ihre dabei verwendeten (Adress-)Daten nur und ausschließlich dafür, dass das Magazin Sie auf dem Postweg sicher erreicht.

Wenn Sie an dieser geübten Praxis nichts ändern möchten, werden wir auch künftig so verfahren. In diesem Fall brauchen Sie nichts zu veranlassen.

Sollten Sie mit der Nutzung für den genannten Zweck allerdings nicht einverstanden sein, müssten Sie uns dieses bitte mitteilen. Wir werden dann Namen und Anschrift im Heftverteiler löschen und Ihnen das DIVSI magazin künftig nicht mehr zustellen.

Möchten Sie von Ihrem Widerrufs- oder Widerspruchsrecht Gebrauch machen, genügt eine E-Mail an info@divsi.de, ein Fax an +49 40 226 36 98 93 oder ein Brief an DIVSI, DIVSI magazin, Mittelweg 110 B, 20149 Hamburg

Darüber hinaus haben Sie die folgenden Datenschutzrechte:

das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit. Ihnen steht auch ein Beschwerderecht gegenüber einer zuständigen Datenschutz-Aufsichtsbehörde zu. Bei Fragen zu diesem Datenschutzhinweis oder Ihren Datenschutzrechten können Sie sich jederzeit unter den obigen Kontaktdaten oder postalisch an uns wenden.

DIVSI

Deutsches Institut für Vertrauen und Sicherheit im Internet