

# Digitale Wirtschaft

*Sie verändert Ökonomie und Gesellschaft, sie treibt die Globalisierung an und setzt analoge Geschäftsmodelle unter Druck. Dem einen ist sie eine Bedrohung, dem anderen die Antwort auf alle Fragen: Die Digitalisierung bleibt mitsamt ihren Auswirkungen auf die Unternehmenswelt Gegenstand hitziger Debatten. Nicht immer sind diese Diskussionen frei von Mythen und Irrtümern. Eine Bestandsaufnahme.*

Von Barbara Engels

## „Erfolgreiche Unternehmen müssen sich nicht mit der Digitalisierung beschäftigen“

**Doch.** Wer langfristig überleben will, kommt an dem Thema nicht vorbei. Richtig ist aber auch, dass nicht für jedes Unternehmen der gleiche Digitalisierungsgrad sinnvoll ist – nicht alle müssen gleichermaßen digital in ihren Prozessen, Produkten und Geschäftsmodellen sein.

Die hohe Erwartungshaltung, was das Potenzial der Digitalisierung angeht, wird stark durch den Erfolg weniger Konzerne bestimmt, den sogenannten MAAMAs: Meta, Alphabet, Amazon, Microsoft und Apple. Sie ist in vielen Fällen überzogen. Ein direkter Vergleich mit den MAAMAs kann unrealistische Erwartungen hervorrufen, denn

tatsächlich unterscheidet sich das Wertschöpfungspotenzial der Digitalisierung von Firma zu Firma erheblich; es hängt sowohl von der Unternehmenskultur als auch seinem Produktangebot und Geschäftsmodell ab.

Wie hoch der Grad der potenziellen Wertschöpfung aus der Digitalisierung ist, hängt davon ab, ob ein Produkt „tangible“, physisch greifbar ist oder nicht. Für tangible Produkte ist er am höchsten, für nicht tangible am niedrigsten. Die Ansatzpunkte für die Digitalisierung eines Lebensmittels, etwa eines Brotes, sind überschaubar – ein Brot bleibt immer ein Brot. Dagegen können andere tangible Produkte, wie etwa Staubsauger, durch den Einbau von Sensoren zu hybriden Produkten werden. Daraus ergeben sich neue Geschäftsmodelle, etwa Pay-per-Use-Ansätze, bei denen der Hersteller dem

Kunden das Gerät zur Verfügung stellt und der Kunde nur für die tatsächliche Nutzung bezahlt.

Die Investitionen, die erforderlich sind, um digitale Wertschöpfung zu betreiben, sind für intangible Produkte am geringsten und steigen über hybride Produkte bis hin zu rein tangiblen Produkten an. Diese Investitionen müssen getätigt werden, bevor sich der Mehrwert ergibt, sie sind, finanzwirtschaftlich gesprochen, „upfront“.

Generell können die Investitionen die erforderliche Infrastruktur, Hardware und Software betreffen. Sie können sich etwa auf den Einbau von Sensoren oder die Erzeugung eines digitalen „Zwillings“ beziehen, die virtuelle Abbildung eines Objekts oder Systems. Kaum zu quantifizieren sind die Kosten für die Investition in die Unternehmenskultur selbst: Je digitaler

# Bild nur in Printausgabe verfügbar

*Zentrum des digitalen Zeitalters: Wenn originär analoge Unternehmen dem Narrativ der Technologiegiganten (hier das Google-Büro in London) nicht blindlings folgen mögen, dann ist das ökonomisch nachvollziehbar.*

diese Kultur ist, desto leichter ist es, das digitale Potenzial zu erkennen und zu heben.

Es ist also nicht für jedes Unternehmen gleichermaßen sinnvoll, in Digitalisierung zu investieren. Dass originär analoge Unternehmen dem digitalen Narrativ von Technologiegiganten wie Google nicht blindlings folgen, ist ebenso verständlich wie ökonomisch sinnvoll. Wie der Königsweg aussieht, muss jede Firma für sich herausfinden: Sie muss experimentieren und prüfen, an welcher Stelle sie digital vorgeht, was sinnvollerweise analog bleibt, und wo sich das Analoge mit dem Digitalen kombinieren lässt. Dazu gehört auch, sich von den Allmachtsfantasien zu lösen, die der Digitalisierung zugesprochen werden. Ein

Sowohl-als-auch, eine hybride Lösung, ist für weite Teile der Wirtschaft – und Gesellschaft – der sinnvollste Weg der Digitalisierung.

Den Kopf in den Sand zu stecken und die Digitalisierung zu ignorieren, kann aber niemals eine Lösung sein. Digitale Lösungen fordern bestehende Geschäftsmodelle heraus, der Wettbewerb wird intensiver – auch, weil er immer internationaler wird. Unerwartete Entwicklungen wie Lieferkettenschwierigkeiten und Preissteigerungen stellen Bestehendes infrage. Unternehmen tun gut daran, ihre Krisenresilienz mithilfe der Digitalisierung zu erhöhen. Trivial ist das nicht, denn die Digitalisierung ist kein einmaliges Ereignis, das mit einem Software-Update

oder der Einführung eines digitalen Produkts erledigt ist, sondern ein fortwährender Prozess.

In welchem Maße etwa die Corona-Pandemie einen Digitalisierungsschub in Deutschland ausgelöst hat, zeigt der Digitalisierungsindex, den das Institut der deutschen Wirtschaft jährlich im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz erstellt. Menschen wie Unternehmen haben gelernt, intensiver digital miteinander zu interagieren. Hinzu kam der Faktor Zeit: Unternehmen mussten den Einsatz digitaler Technologien in kürzester Zeit umsetzen, um diese Krise zu überstehen.

Andererseits wurden auch digitale Projekte in der Krise aufgrund von Unsicherheiten, Kostendruck und Liquiditäts-

problemen vertagt. Inzwischen stagniert die Digitalisierung der deutschen Wirtschaft wieder. Auch das könnte der weiter bestehenden und mittlerweile multiplen Krise geschuldet sein: Zu den Auswirkungen der Corona-Pandemie haben sich die Folgen des Ukraine-Krieges, die Lieferkettenschwierigkeiten, die Preisentwicklung und die Energiekrise gesellt.

Die Digitalisierung wird vermutlich erst dann richtig an Fahrt aufnehmen, wenn die Unternehmen weniger unter dem Eindruck von Kostensteigerungen und Unsicherheiten stehen. Spätestens dann jedoch hat wirklich kein Unternehmen mehr eine gültige Ausrede, nicht zumindest zu prüfen, inwiefern Digitalisierung ihm nützt.

---

### „Aber alles, was digital vernetzt ist, kann digital angegriffen werden“

**Das ist leider wahr.** Es ist nicht die Frage, ob ein Unternehmen, eine Institution, ein Privatschiff digital angegriffen wird, sondern wann und wie oft es geschieht – und wann das Opfer den Angriff bemerkt. Cyberangriffe finden jederzeit statt und können jeden treffen – und sie werden auch jeden treffen. Laut dem Branchenverband Bitkom haben Cyberangriffe bei 86 Prozent der Unternehmen in Deutschland in den Jahren 2020 oder 2021 einen Schaden verursacht. Die Schäden durch Ransomware-Angrif-

fe – also durch Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln –, verbunden mit dem Ausfall von Systemen oder der Störung von Betriebsabläufen, sind laut Bitkom seit 2019 um 358 Prozent gestiegen.

Cyberangriffe sind für die Angreifer ausgesprochen attraktiv, weil sie ortsunabhängig verübt werden können und keine größeren personellen, zeitlichen oder finanziellen Ressourcen beanspruchen. Cyberkriminelle suchen systematisch nach Schwachstellen in IT-Systemen und nutzen sie zur Gelderpressung oder anderen Zwecken. Eine kleine Sicherheitslücke genügt, um ein ganzes System über Wochen oder Monate lahmzulegen.

Dabei müssen die Systeme nicht einmal zielgerichtet attackiert werden – es reicht ein automatisierter Angriff per Gießkannenprinzip. Das trifft vor allem kleinere Unternehmen, die oft geringe Sicherheitshürden haben und niemanden, der sich um die IT-Sicherheit kümmert. Solche Firmen werden gerne als Einfallstor genutzt, um großen Unternehmen oder Regierungsinstitutionen zu schaden, die mit den kleinen Firmen vernetzt sind, etwa im Rahmen eines Zuliefererverhältnisses.

Die Angriffsmethoden und Angriffswerkzeuge sind in den vergangenen Jahren immer vielfältiger und ausgeklügelter geworden. Die Phishing-Mails, mit denen Hacker versuchen, Malware auf fremden Rechnern

zu installieren, sind längst nicht mehr auf den ersten Blick als solche erkennbar. Auch die Zahl der Angriffspunkte hat sich dramatisch erhöht: Seit der Corona-Pandemie arbeiten viele Menschen vermehrt aus dem Homeoffice. Häufig sind die Netzwerke daheim nicht so gut geschützt wie die des Unternehmens.

Besonders gern nutzen Hacker die „Schwachstelle Mensch“: Sind wir unaufmerksam, neugierig oder arglos, können Angreifer besonders leicht über einen nebenbei geöffneten Email-Anhang oder einen beiläufig geklickten Link in IT-Netzwerke eindringen. Und dann wird's teuer: Cyberangriffe können gerade für kleine Firmen existenzbedrohend sein.

Aber auch größere Unternehmen trifft ein wochenlanger Ausfall von Systemen hart. Die Kosten der Betriebsunterbrechung können schnell in die Millionen gehen, sei es wegen Produktions- und Umsatzausfällen, wegen Schäden an der Betriebsausstattung oder aufgrund von Image-Einbußen.

Allerdings sind wir dieser Entwicklung nicht vollkommen ausgeliefert. Wir können uns vor Hackerangriffen schützen, indem wir Cybersicherheit als Ziel jedes Unternehmens und jeder Institution festschreiben und klug darin investieren. Das ist nicht trivial, denn Cybersicherheit hat ein Sichtbarkeitsproblem. Wenn sie da ist, fällt sie nicht auf. Wenn sie nicht da ist, wird es schmerzhaft. Eine Investition in Sicherheit hat kein direkt quantifizierbares

Ergebnis. Weder steigt der Umsatz messbar, noch kann jeder verhinderte Cyberangriff identifiziert und als Erfolg verbucht werden.

Hinzu kommt, dass es nicht mit einer einmaligen Investition getan ist. Cybersicherheit ist ein kontinuierlicher Prozess, der ständige Aufmerksamkeit erfordert. Ein hundertprozentiger Schutz ist dabei nicht erreichbar. Umso wichtiger ist es, dass IT-Systeme solche Angriffe gut auffangen können und sich schnell wieder davon erholen. Die Antwort auf digitale Bedrohungen lautet Cyber-Resilienz. Generell gilt: Prävention ist besser als Reaktion – und günstiger.

Die Digitalisierung mit all ihren Vorzügen wird weiter voranschreiten. Das ist gut so. Wenn wir aber die Cybersicherheit vernachlässigen, werden wir nie das volle Potenzial der Digitalisierung ausnutzen können. Mehr noch: Im schlimmsten Fall werden nicht nur Digitalisierungsprojekte scheitern, sondern wird auch die Sicherheit von Wirtschaft und Gesellschaft unterminiert. Das gilt umso mehr, seit Cybersicherheit zu einem geopolitischen Faktor geworden ist. Nicht nur der Ukraine-Krieg wird auch im digitalen Raum ausgetragen.

---

### „Daten sind das neue Öl der digitalen Wirtschaft“

**Der Vergleich wird gern angestellt, aber er hinkt.** Ebenso gut können wir Daten mit Son-

nenlicht oder mit Infrastruktur vergleichen.

Mit dem Öl ist den Daten gemein, dass sie veredelt werden müssen, um einen Mehrwert zu bringen: bereinigt, analysiert, kombiniert. Wie Öl werden bestimmte Daten samt den Erkenntnissen, die sie liefern, in großem Stil gehandelt. Das dominierende Geschäftsmodell der digitalen Welt basiert auf Onlinewerbung und die wiederum auf dem Handel mit personenbezogenen Daten. Anders als Öl werden aber gerade maschinengenerierte Daten nur begrenzt gehandelt, denn die meisten dieser Daten, die vor allem in Unternehmen anfallen, bleiben ungenutzt. Sie werden zwar erhoben, aber nicht weiterverarbeitet oder gar mit anderen Unternehmen geteilt.

Vergleichen wir also Daten mit Sonnenlicht – einem öffentlichen Gut. Wie Sonnenlicht sind Daten überall und unterliegen allem. Gemäß der Open-Data-Bewegung sollten Daten auch für alle da sein und von allen genutzt werden können. Denn ebenso wie Sonnenlicht gibt es genug Daten für alle – sie verbrauchen sich nicht. Daten umfangreich und zu verschiedenen Zwecken zu nutzen, kann den Wohlstand steigern.

Allerdings gibt es rechtliche Vorgaben, welche die umfassende Nutzung von Daten aus guten Gründen einschränken. Menschen haben ein Recht darauf, dass ihre Daten und damit ihre Privatsphäre geschützt werden. Unternehmen sehen kaum Anreize, ihre Daten zu teilen. Im Zwei-

felsfall haben sie Angst, dass ihre Daten zu viel über ihr Geschäftsmodell und ihre Prozesse verraten. Das liegt auch daran, dass viele Unternehmen gar keinen Überblick darüber haben, welche Daten sie bedenkenlos teilen können und welche nicht.

Der Vergleich von Daten mit Infrastruktur liegt insofern nahe, als Daten grundlegend sind für die Organisation von Wirtschaft und Gesellschaft. Wie Infrastruktur – etwa Straßen – brauchen sie Investitionen, Pflege und Management. Das erfordert nicht nur entsprechende Technologien, sondern auch Regeln, Strukturen und Institutionen, welche die Interessen von Datenproduzenten und Datenutzern miteinander abgleichen.

Letztlich hinkt jeder dieser Vergleiche. Welcher der passendste ist, hängt von unserem Blickwinkel auf Daten und die Datenökonomie ab – und der ist geopolitisch geprägt.

In den USA werden Daten wie Öl behandelt. Daten sind privatisiert: Wer sie gewinnt, dem gehören sie auch. Diese privaten Datenschätze sind das Erfolgsrezept der amerikanischen Digitalwirtschaft. Dank ihrer konnten Unternehmen wie Google oder Facebook entstehen, die erhebliche Mengen von Daten sammeln, auswerten und für sich nutzen. In den Vereinigten Staaten gilt das Prinzip der Marktfreiheit, mit regulatorischen Eingriffen hält man sich zurück. Statt vorausschauend Datenschutz und Wettbewerb zu

# Bild nur in Printausgabe verfügbar

*Kontrolliert und durchnummeriert: Daten werden in China als strategische ökonomische Ressource des Staates gesehen, mit deren Hilfe sich politische Stabilität und Sicherheit im Sinne der Regierung gewährleisten lassen.*

regulieren, werden Probleme per Gerichtsverfahren geklärt. Dementsprechend ist Datenschutz auch kein Grundrecht, sondern eine Selbstverpflichtung der Unternehmen.

Zwar gibt es in einzelnen Bundesstaaten eine Datenschutzregulierung, etwa den California Consumer Privacy Act, aber es gibt keinen harmonisierten Datenschutz auf Bundesebene. Das fällt den USA derzeit auf die Füße. Sie haben es verpasst, Vorreiter in Sachen Datenschutz zu sein und international Standards zu setzen. Deshalb müssen sie sich nun an internationale Regulierungen wie die Europäische Datenschutzgrundverordnung (DSGVO) anpassen.

In China werden Daten wie Sonnenlicht gesehen – allerdings scheint diese Sonne nicht für alle. Die Daten gehören letzten Endes dem Staat. Er kontrolliert sie, er führt sie zusammen und stellt

sie bereit, wenn es ihm sinnvoll erscheint. Daten sind also eine strategische ökonomische Ressource für den Staat. Sie sollen politische Stabilität und nationale Sicherheit im Sinne der Regierungspartei gewährleisten.

Entsprechend schützt die Regulierung in China die Daten von Menschen gegebenenfalls vor dem Zugriff von Unternehmen, nicht aber vor dem Zugriff des Staates. Die Regulierung ist eine Kombination aus Rechten für den Staat, Pflichten für die Unternehmen und wenigen Rechten für Individuen. Vermittels seiner Kontrolle über die Daten überwacht der Staat Wirtschaft und Gesellschaft und schottet den heimischen Markt ab.

Der europäische Weg unterscheidet sich grundlegend vom libertären Modell der USA und dem autoritären Chinas. In Europa werden Daten am ehesten als eine Infrastruktur gesehen,

die Institutionen und Regeln benötigt, um die optimale Nutzung der Daten im Sinne von Wirtschaft und Gesellschaft zu ermöglichen. Datenschutz und das Recht auf informationelle Selbstbestimmung gelten als Grundrechte. Regulierungen sollen einen Ausgleich zwischen dem Schutz der Konsumenten und der Wettbewerbsfähigkeit der Unternehmen herstellen.

Ziel ist eine Balance zwischen dem Schutz personenbezogener Daten und der Gestaltung eines freien Datenverkehrs im Binnenmarkt – ein rechtssicherer Raum, der Innovationen anregt und Wettbewerb ermöglicht. Ein so komplexes Ziel bringt komplexe Regeln mit sich – darunter die DSGVO, den Digital Markets Act, den Digital Services Act und den Data Act. Daten und die Datenökonomie sind komplex – und keineswegs einfach nur wie Öl.

## „Die Digitalisierung ist ein Klimakiller“

**Jein.** Zwar hat die Digitalisierung nicht nur positive Auswirkungen auf Klimaschutz und Nachhaltigkeit. Aber sie als Klimakiller zu bezeichnen, tut ihr Unrecht. Denn die Digitalisierung ist ein wichtiges Mittel, um Nachhaltigkeit zu erreichen.

Dieser Zusammenhang spielt nicht nur national eine immer größere Rolle, etwa bei der Deutschen Nachhaltigkeitsstrategie, dem Ressourceneffizienzprogramm und in der umweltpolitischen Digitalagenda, sondern auch auf europäischer Ebene, etwa im Rahmen des EU Circular Economy Action Plans. Auch auf der Plattform des Bundesministeriums für Bildung und Forschung (BMBF) „Forschung für Nachhaltigkeit“ werden Digitalisierung und Nachhaltigkeit zur Umsetzung der Agenda 2030 konsequent zusammengedacht.

Wenn Daten in großem Maßstab genutzt werden, wenn Vernetzung stattfindet, wenn Automatisierung und Autonomisierung an Bedeutung gewinnen, dann kann all das zu Umwelt- und Klimaschutz beitragen, und es kann dabei helfen, die Ressourcen- und Energieeffizienz in Industrie, Landwirtschaft, Gebäuden und Transport zu steigern. Andererseits kann es auch zu einem gesteigerten Ressourcen- und Energieverbrauch führen.

Direkte negative Effekte der Digitalisierung auf die ökologische Nachhaltigkeit entstehen

vor allem durch den Energiebedarf und die Treibhausgasemissionen beim Betrieb und bei der Herstellung von digitalen Endgeräten und Infrastrukturen sowie durch Abfälle und langlebige anthropogene Schadstoffe. Gerade der Ressourcenverbrauch der Datenspeicherung und -verarbeitung wird häufig unterschätzt.

Indirekte negative Effekte ergeben sich aus der Veränderung bestehender Produktions- und Konsummuster, die aus der Anwendung digitaler Technologien resultieren. So werden Produkte und Dienstleistungen qualitativ besser und gleichzeitig preiswerter, sodass sie stärker nachgefragt werden. Die hohe Dynamik der Digitalisierung führt außerdem zu dem, was die Wirtschaftswissenschaftler als „Obsoleszenz“ bezeichnen: Die Güter und Produkte veralten, könnten zwar noch länger genutzt werden, werden jedoch hardware-, software- oder psychologisch bedingt obsolet.

Wenn dank größerer Effizienz die Kosten für Produkte oder Dienstleistungen sinken, dann kann das dazu führen, dass sich das Verhalten der Nutzerinnen und Nutzer ändert. Sie verbrauchen mehr, wodurch die ursprünglichen Einsparungen teilweise wieder aufgehoben werden: der sogenannte Re-

bound-Effekt. Auf die Frage, ob der Energieverbrauch insgesamt durch Digitalisierung steigt oder fällt und welche Effekte die Digitalisierung auf die Ressourceneffizienz haben kann, lässt sich nach den vorliegenden Studien keine eindeutige Antwort geben.

Der ehemalige Präsident der „Society for the History of Technology“ Melvin Kranzberg bringt die Ambivalenz von Digitalisierung auf den Punkt, wenn er sagt, Technologie sei „weder gut noch böse. Neutral ist sie aber auch nicht.“ Technologie und damit auch Digitalisierung sind nur so unparteiisch wie die Menschen, die sie erschaffen und nutzen. Digitalisierung kann sehr nachhaltig, aber auch ausgesprochen un-nachhaltig wirken.

Die technische Entwicklung allein ist für eine nachhaltige Entwicklung notwendig, aber nicht hinreichend: Sie muss in einen sozio-ökonomischen, sozial-ökologischen, sozio-politischen und sozio-kulturellen Kontext gesetzt werden, der die positiven Auswirkungen der Digitalisierung forciert und die negativen minimiert. Es sind die Menschen, die es in der Hand haben, wie sich Digitalisierung auswirkt und wie sie so gestaltet werden kann, dass Wirtschaft und Gesellschaft nachhaltig von ihr profitieren.



**Barbara Engels**

ist Senior Economist für nachhaltige Digitalisierung beim Institut der deutschen Wirtschaft in Köln.